Tap That

A Gentle Introduction to Hacking Hardware

By

Kevin Finisterre & Josh Thomas

Special Guest star: Nathan Keltner

Time for that pimp sauce...

The same thing we do every night...

http://en.wikipedia.org/wiki/Pinky_and_the_Brain
http://www.youtube.com/watch?v=iJPFSNu_QNs

Class Overview: D1.1

- Building a Lab @ Home
- EE Basics and You
- Lab 1: Taking things apart
- JTAG, ICE, SPI & other Acronym Soup
- Lab 2: Talking to things
- Blob o' Junk
- Lab 3: Runtime Analysis

Class Overview: D1.2

- Soldering all the things
- Lab 4: To Live and Die in LA
- Stories from a Real Life Fab project
- Lab 5: We are persist, now what?
- Techniques for moving beyond n00b
- Lab 6: A dash of pwn sauce...

First Half Schedule

- Building a Lab @ Home
- EE Basics and You
- Lab 1: Taking things apart
- JTAG, ICE, SPI & other Acronym Soup
- Lab 2: Talking to things
- Blob o' Junk
- Lab 3: Runtime Analysis

Welcome to Class

I’m KF

I can’t speak for the other guys, but I am very interactive. Feel free to interrupt me, correct me, call bullshit and ask questions where ever you see fit. If you need clarification just ask...

If you ever want to troll KF... fill a slide deck with random google images pics.... sorry brother :p

I’m JT

don’t listen to me, ask me for help... interrupt me a bunch... i babble like a mad man

I’m NK

plz to NK here

Who are you?

plz to NK here

What are our Goals?

- Dump all the firmwares
- Write all the firmwares
- Pwn all the devices
- Break all the things

plz to JT here

Building a Lab @ Home

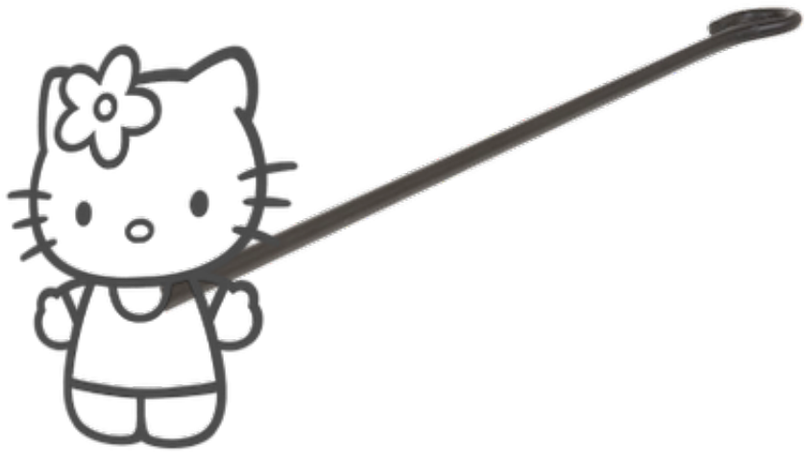
plz to JT here

This man had a dream! http://blog.crashspace.org/2010/04/magical-unicorns/
Sibblings - http://www.flickr.com/photos/crashspacela/5168388113/in/photostream/
Pwnsauce - http://www.flickr.com/photos/crashspacela/5163143089/in/photostream/

Tools to get you started

- Selecting an Iron
- Selecting a HotAir Station ?
- Other build gear
- Saleae and other Logic Analyzers
- Hardware for Hardware people
- Software for Hardware people

plz to JT here



I can haz iron?

“New memes are added to the top, feel free to share them” - http://moonsisters.org/PhotoZ.html
Hello Kitty Branding Iron - http://www.moonsisters.org/moonsisters/ChairShotZ/September2012/hellokittycattleprod.png

Requirements

- Basic:
  - Does it get hot?
- Advanced:
  - Can you control how hot it gets?
  - Can you change the tip?
  - Does it make you happy inside?

Make sure that your Iron tastes like burning... http://www.youtube.com/watch?v=U5deItDV0k8
Just the Tip? - http://www.troll.me/images/rape-sloth/cmon-baby-just-touch-it-just-the-tip.jpg

n00b iron

- The Radio Shack 40-Watt Pencil Iron
- It does get hot... at least eventually
- Everyone starts here... don't be ashamed
- Honestly not as bad as JT is making it out to be

http://www.radioshack.com/product/index.jsp?productId=2062738
Model 64-2071

#boss Iron

- Weller WESD 51 - All the digitals
- Weller WES 51 - Analogue for the skinny jeans types
- Damn good iron
- Not too expensive
- Ebay FTW!

http://www.mouser.com/ProductDetail/Weller/WESD51/?qs=0lHHbjvaHISJj5Nu2r8YCg==
http://www.amazon.com/Weller-WESD51-Digital-Soldering-Station/dp/B000ARU9PO

#boss Iron

- MetCal MX-500p
- Stupid Expensive
- Best Iron EVAR!
- Probably don't need this.
- Ebay FTW!

Colin O'Flynn @colinoflynn 13 Sep
@m0nk_dot @danielbuentell0 @joegrand I would sell my soul before my Metcal. Can switch from 0402 to SMA on gnd plane youtu.be/3yrGukOttZY
Joe Grand @joegrand 13 Sep
@m0nk_dot @danielbuentell0 @colinoflynn Yeah, I have a Metcal MX-500P. Love it almost as much as my oscilloscope ;)
View conversation

http://www.digikey.com/product-detail/en/MX-500P-11/MX-500P-11-ND/427653
http://www.amazon.com/Metcal-Power-Supply-MX-500-Switchable/dp/B000PDOZ8A

Realistic Suggestions

- Hard to go wrong with Weller
- Hakko is also loved
- You pay for quality

Wellwer WM120 - http://www.amazon.com/Weller-WM120-120v-Pencil-Soldering/dp/B0000WT586
Hakko FX-951 - http://www.amazon.com/AMERICAN-HAKKO-PRODUCTS-INC-FX-951/dp/B0012B8NW8

Today's Menu

- We actually use these
- Carry on an airplane
- Gets hot, melts stuff
- USB!
- Runs off 9Volt battery in an emergency

I first noticed USB Soldering irons emerge within the circuit bending scene... - http://www.getlofi.com/?page_id=1934
You can get it from Megatone because GetLoFi is ALWAYS sold out, you want the "MEGA POWER" MSD-085 - http://www.megatone.com.tw/Products/SubCategory/4/MegaPower®%20Tools/83/USB%20Precision%20Soldering%20Iron/
The -001, -002, -003 variants allow you to purchase the iron WITH a USB, Cable, 9Volt battery cable, or both.
The newer MSD-086 can be found all over amazon and most random electronics suppliers.
http://www.jameco.com/Jameco/catalogs/c133/P136.pdf
http://www.amazon.com/MEGATONE-ELECTRONICS-CORP-Portable-Soldering/dp/B00C9NWR4I

Care and Feeding

Don’t Do that

- Clean your Iron with an X-Acto knife

So... these are all used
to build stuff

But I want to break
things!

plz to JT here

MultiUse Stations

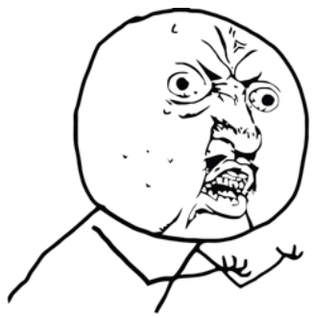
- It's all just hot air anyway....
- Why solder on chips when you can desolder them?
- Trade high quality for functionality

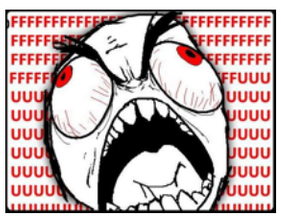
Quick Clip of KF torching a flight controller with a heat gun (from home depot) - http://www.youtube.com/watch?v=oXuw9E5XiWc
Hey I found an easter egg!

One device to rule them all?

This is my DREAM all in one (KF) - http://www.amazon.com/WR3000M-Digital-Self-Contained-3-Function-Tools/dp/B0019V5PSQ/ref=pd_sxp_f_r#productDetails
One man bands for the win! - http://www.youtube.com/watch?v=uXMuWi0dUBc
I know one of you are gonna troll me and ask what printer that is (Stephen Hilt)! - http://www.brother-usa.com/MFC/

Pls to not rage now





Y U NO ALL IN ONE!@#@#$ - http://lmgtfy.com/?q=rageface

ReWork not Re:Work

- No more metal on metal action
- Hot air + fan = disassembly
- Brands mean less here
- More about functionality

The above station is a unknown clone “850/852 series” hot air station. It is nearly identical to the Sparkfun 303D model.
There are hundreds of clones of this 8xx style hot air station. Seriously... search any .cn distributor.
Sparkfun Hot-air Rework station - 303D https://www.sparkfun.com/products/10706
Plus models are very popular as they combine an iron. http://www.goodluckbuy.com/best-852d-lead-free-hot-air-gun-with-helical-wind-rework-station.html
I personally have to bang on my Sparkfun model to get it to cool down. I suspect a bad thermocouple.
I’m not into random .cn hardware that gets reallllllly hot. Be careful... you have been warned. Keep an eye on these things. They may burn your house down!

Now in Pwnium Silver!

JT: My old one was the black one above. Great until the hot air gun plastic melted. Had a bunch of knobs and some temp readouts... never figured out the manual as it was in Chinese... side note, honestly a good iron attached.
SMTMAX 8502 2-in-1 Hot Air Rework Soldering Station - http://www.amazon.com/8502-Hot-Rework-Soldering-Station/dp/B0051PXTXY
Aoyue 2702A+ SMD Professional Repair & Rework Station - http://www.amazon.com/Aoyue-Profesional-Repair-Rework-Station/dp/B000HDJ5J2

Baaaaaaaaalllllllin!

- WR3000 == BonerTown
- Comes with Hot Air
- Desoldering tool!
- LCD for non hipsters

The Weller WR3000M digital self-contained 3 function rework station with tools is a versatile repair station that's specifically tailored to the needs and requirements of professional repairs, to the latest technology electronic sub-assemblies in industrial productions engineering, and in the repair and laboratory fields. The rework station includes the WR3M soldering station, HAP200 (200 watt) hot air pencil, WP80 (80 watt) soldering iron, and the DXV80 (80 watt) desoldering iron. The WR3M's power supply is 120 volts and power consumption is 400 watts. Temperature ranges from 150 Degree F to 999 Degree F. The hot air pump has an on/off duty cycle of 30 seconds with a hot air maximum capacity of 15 l/min. The vacuum pick up pump has an on/off duty cycle of 60 seconds on and 30 seconds off. The WR3M's automatic tool detection guarantees the simultaneous operation of all 3 soldering tools. Made in Germany.
^------ Drooling
http://www.amazon.com/WR3000M-Digital-Self-Contained-3-Function-Tools/dp/B0019V5PSQ/ref=pd_sxp_f_r#productDetails

JT's Basement of Quirky Toys

JT: This thing was awesome, for the 10 minutes it worked. Burned 2 goodFets, then it died. :/ (about $125 on eBay)
Puhui IT T862 MACHEEEEN - http://www.puhuit.com/main/page_products_t862_bga_station1.html
How to use the T-862++ Digital Infrared IRDA Soldering station - http://www.youtube.com/watch?v=RrA-trDZPNs
The one above has a knob on it, so is likely yet another clone.

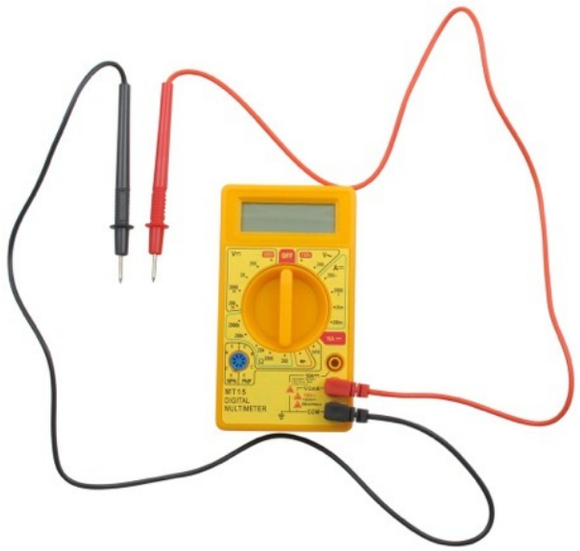
Final Options

Look into the Sparkfun tutorials if you want to head this route, they also have a controller for more precise control - https://www.sparkfun.com/products/retired/81
The infamous 2006 Sparkfun Reflow Toaster tutorial - https://www.sparkfun.com/tutorials/60
KF has been known to run to Target in emergency situations to rock out the 12" Hinged Oster Skillet - http://www.target.com/p/oster-12-hinged-lid-skillet-black/-/A-10990114

That is seriously an impossible to find $200 vintage Hello Kitty oven BTW@! http://compare.ebay.com/like/121115009513?var=lv&ltyp=AllFixedPriceItemTypes&var=sbar

MultiMeter!

- What's going on?
- Where does that go?



What NOT to do with a Multimeter from a EE - http://electronics.stackexchange.com/questions/34229/what-not-to-do-with-a-multimeter

Moar MultiMeters!

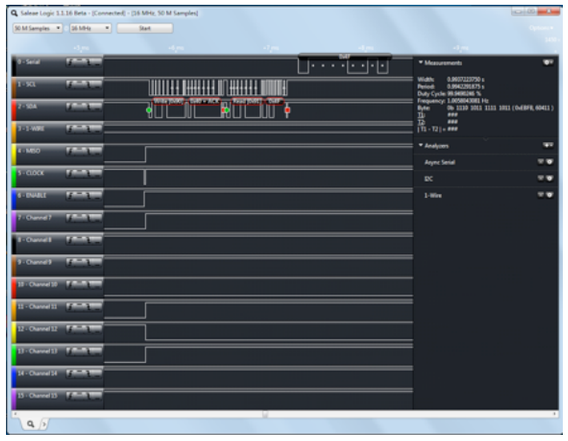
- The price jumps here are HUGE
- The functionality... not so much

KF rocks an old school Radioshack 22-810 - http://support.radioshack.com/support_meters/doc66/66016.pdf
It seems to have been replaced by a more hipster Pocket version the 22-820 - http://www.radioshack.com/product/index.jsp?productId=2104114

Other one is an overpriced FLUKE 87V @ ~$320

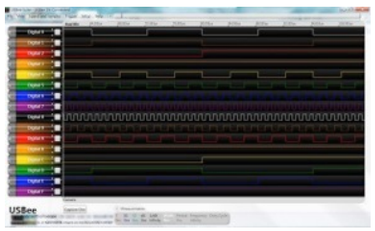
Logic & Analysis

- If you only buy one thing...



Lets get this clear right off the bat... “Say-lee-’A’”, Having said that... I call mine a “suh lay” and I think most of my friends do too.
http://www.saleae.com/logic/faq
I discovered it in 2010... been in love ever since - http://www.digitalmunition.com/_/Blog/Entries/2010/11/25_Say_what_Lets_try_Say-lee-A_as_in_Saleae.html
Back in the day it was just the 8 channel http://www.saleae.com/logic
Now you should get the 16 or GTFO! http://www.saleae.com/logic16

If you just have too much $$$

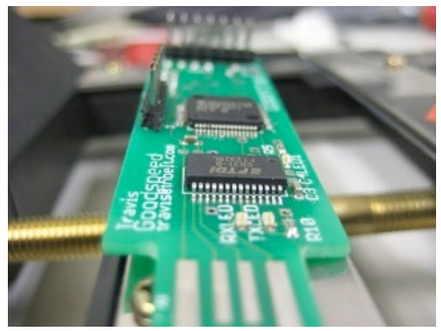


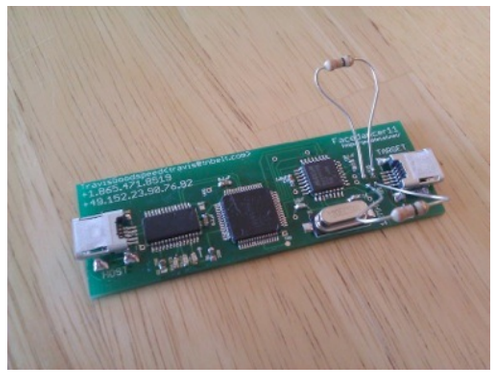
If you have 3 grand to burn or can get your office to expense it, got for one of these I guess!
http://www.usbee.com/qx.html

Hardware Reversing Toolkit

plz to JT here

The illustrious neighbor

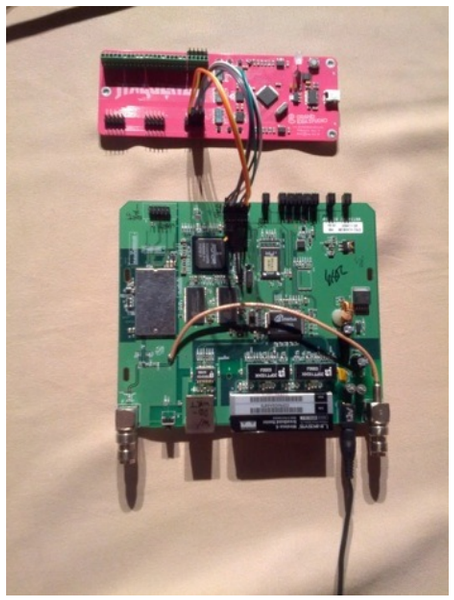




The now infamous Kees Cooks Facedancer - http://www.outflux.net/blog/archives/2013/01/21/facedancer-built/
What on earth is Trav holding? - http://www.radiantmachines.com/category/belt-buckles/
http://www.flickr.com/photos/travisgoodspeed/3044198752/

Joe Goes METAL

- Tap everything
- Parallax finds JTAG
- You relax



http://www.grandideastudio.com/portfolio/jtagulator/
http://www.youtube.com/watch?v=uVlsbXzQOIU
http://www.parallax.com/product/32115
https://github.com/grandideastudio/jtagulator
https://www.defcon.org/images/defcon-21/dc-21-presentations/Grand/DEFCON-21-Grand-JTAGulator.pdf

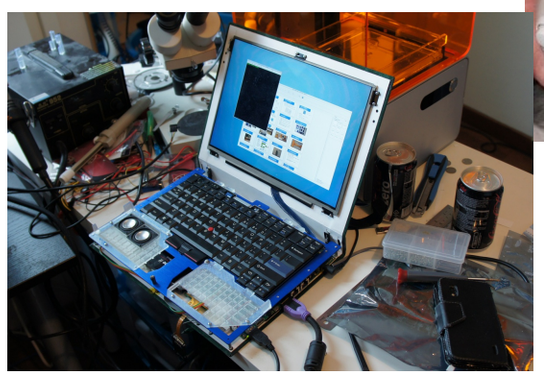
DIY Hero

- Mike Ossmann

A memetic legend is born.... http://ossmann.blogspot.com/2010/03/16-pocket-spectrum-analyzer.html
Expand on the neighborly theme, give your hommies tools - http://greatscottgadgets.com/hackrf/

Don’t Forget Bunnie

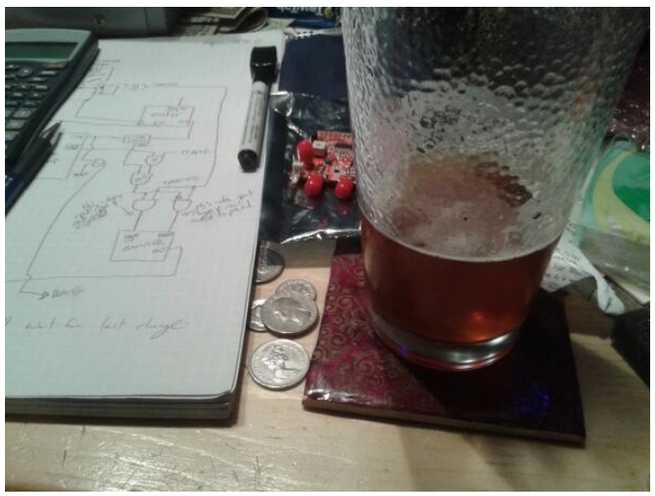
- I all the xBoxes?
- Maybe a laptop?



If you don’t have a hard copy of “Hacking the Xbox on your book shelf, be ashamed. - http://www.amazon.com/Hacking-Xbox-Introduction-Reverse-Engineering/dp/1593270291
If you don’t have the digital copy... stand up and leave right now - http://nostarch.com/xboxfree
Free ebooks from Bunnie! - http://www.bunniestudios.com/blog/?p=3012
Andrew == Bunnie? yerp http://en.wikipedia.org/wiki/Andrew_Huang

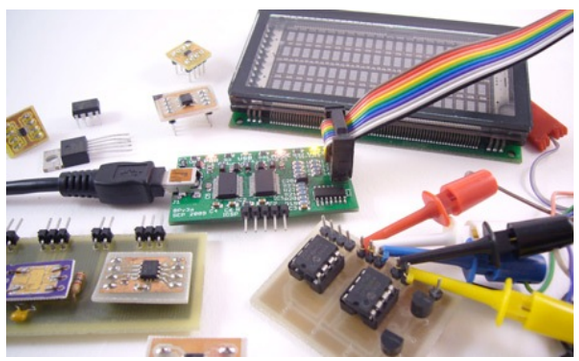
Collin is Moving on Up

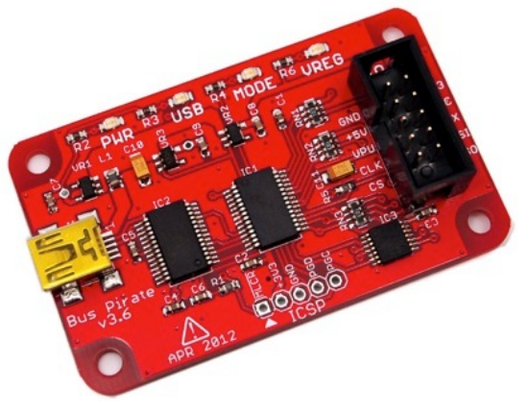
- Side channel attacks for poor hackers
- Canadian = Nice Guy



If you don't have a hard copy of "Hacking the Xbox on your book shelf, be ashamed. - http://www.amazon.com/Hacking-Xbox-Introduction-Reverse-Engineering/dp/1593270291
If you don't have the digital copy... stand up and leave right now - http://nostarch.com/xboxfree
Free ebooks from Bunnie! - http://www.bunniestudios.com/blog/?p=3012
Andrew == Bunnie? yerp http://en.wikipedia.org/wiki/Andrew_Huang

Pirates and Shit



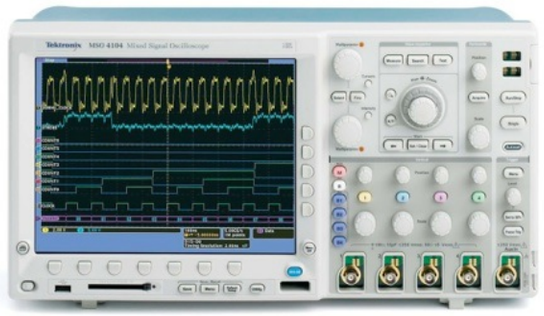


Sparkfun - https://www.sparkfun.com/products/9544
SeeedStudio - http://www.seeedstudio.com/depot/bus-pirate-v36-universal-serial-interface-p-609.html
Mind the brand & cable pinout! - http://dangerousprototypes.com/docs/Common_Bus_Pirate_cable_pinouts
General project info - http://code.google.com/p/the-bus-pirate/

Fresh as Hell

You gotta bro! The Fedz watchin... http://www.youtube.com/watch?v=NttlPwNKd_M

The o-face



Oscium is an interesting Oscilliscope for the i* devices - http://www.oscium.com/products/mixed-signal-oscilloscope-imso-104 (not pictured above)
The Tektronix 515A is a circa 1960s style museum piece - http://www.radiomuseum.org/r/tektronix_oscilloscope_515a515.html
Now back to THIS decade, if you have a spare 8-20 grand you can pick up a Tektronix MSO4104 - http://www.tek.com/oscilloscope/mso4000-dpo4000

More crap from JT's lab

At some point your should probably man up and buy an Agilent Tech power supply such as the E3630A shown in this slide - http://www.home.agilent.com/en/pd-838235-pn-E3620A/50w-dual-output-power-supply-two-25v-1a?&cc=US&lc=eng or the smaller scale E3610A - http://www.home.agilent.com/en/pd-838240/30w-power-supply-8v-3a-or-15v-2a?&cc=US&lc=eng (both are discontinued models btw)... EBAY!

Tools the people with real jobs use

plz to JT here

Segger

Fun facts about SEGGER... they KNOW they have a piracy problem and openly discuss it. - http://www.segger.com/jlink-software.html?step=3&file=JLink_442b

Total Phase

Travis Goodspeed
@travisgoodspeed
Follow

.@AA55h I use the @totalphase tools for that. Worth every penny.

Reply Retweet Favorite ••• More

1 FAVORITE

11:43 AM - 31 Dec 12

Travis claims they are worth every penny.... https://twitter.com/travisgoodspeed/status/285833695284326400
KF is too poor...
JT makes sexy time to USB ports with his.
Travis using one of his many Total Phase devices to sniff SPI - http://travisgoodspeed.blogspot.com/2009/03/breaking-802154-aes128-by-syringe.html
Several protocols available.

I don’t want a real job,
just ~#

Real jobs have budgets and like to buy tools... we like to hack the crap out of stuff on the cheap.

“Oriental” Express - Doppelgangers

FREE SHIPPING New ARM Emulator USB JTAG Realview Ulink2 II Debug Adapter ckm

From Hong Kong

1d 11h left
Friday, 12AM

$22.99
1 bid

Free shipping

J link V8 ARM Emulator ARM7 ARM9 ARM11 Cortex-M3 ADS IAR STM32 JTAG Interface

From China

$13.69
Buy It Now

Free shipping

If you are into ARM debugging Segger clones are a dime a dozen as mentioned above the company has a known problem - http://www.ebay.com/itm/J-link-V8-ARM-Emulator-ARM7-9-11-Cortex-M3-ADS-IAR-STM32-JTAG-Interface-TVS-FUSE-/290964067970?pt=LH_DefaultDomain_0&hash=item43becf5682

The RealLink is a similarly hot item for ARM based debugging. - http://www.ebay.com/itm/FREE-SHIPPING-New-ARM-Emulator-USB-JTAG-Realview-Ulink2-II-Debug-Adapter-ckm-/400574441266?pt=LH_DefaultDomain_0&hash=item5d4418e732

Solder + Disposables!

- Talk about shitty lead bearing solder...
- Rosin core?
- Diameter? Size does matter. Like it thick?
- I prefer silver bearing .015 from Rat Shack
- Desolder? Flux?Tinning?
- Tiny tiny wires!@#$
- Beer!
- ChipQuick
- Other stuff? Helping Hands? Tweezers?

Binary Brew Works

D.T S//ASH

Try the d0tslash beer! - http://www.10101brew.com/beer.html

Silver Bearing Solder - http://www.radioshack.com/product/index.jsp?productId=2062725
.015 diameter
64-035

Desoldering Braid
64-2090E
http://www.radioshack.com/product/index.jsp?productId=2062744

Tip Tinner/Cleaner Compound (0.5 Oz.)
http://www.radioshack.com/product/index.jsp?productId=2062721
64-020D

Tweezers
Masking Tape
(tape small fucking wires down!!@#@$#)

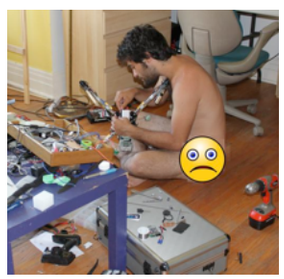
Helping hands... (I never understood em and thought they were dumb) _ I still rm -rf the magnafying glass and iron holder.
64-079
http://www.radioshack.com/product/index.jsp?productId=3928375

30AWG wire
http://www.gcelectronics.com/order/product_search.asp
Part #: 12-630
WIRE WRAP BLUE 30AWG 100 FT

Real Talk

- You need a decent iron
- You need a screw driver
- You need pants

WHY ARE YOU NAKED?
ONE MUST TAKE DRASTIC MEASURES TO PREVENT STATIC DISCHARGE. CARE MUST BE TAKEN TO PRESERVE THE PURITY OF THESE COMPONENTS.
© 2001 Fred Gallagher, all rights reserved.
01.22.2001



Yes... I've soldered without pants. NO I am not the only one! http://diydrones.com/profiles/blogs/how-not-to-work-on-your-quad
Megatokyo anyone? http://megatokyo.com/strip/70

JT: Damn i miss the oldschool MT...

OK, but I'm a software person... when will this make sense?

Software for Hardware People

Most hardware seems like software 10 years ago... plenty of stupid sauce to go around.

SfHP: General Tools

- IDA / Hopper / 010 Editor
- Radare assembler / disassembler
- Binwalk / file (libmagic based code)
- some abandoned python project (HashID?)
- random abandoned ruby project (rbkb?)

Open your wallet here for IDA - https://www.hex-rays.com/products/ida/index.shtml & http://www.ccso.com/licenserules.html
Hopper is a fairly new kid on the block - http://www.hopperapp.com
Radare - http://radare.org/y/
Binwalk has had a full rewrite in Python as of v1.0 - http://code.google.com/p/binwalk/
The auto extract is something you should be aware of.
Hash anyone used HASHiD? https://github.com/psypanda/hashID/blob/master/python/hashid.py
At least you have *heard* of RBKB from Matasano? https://github.com/emonti/rbkb

SfHP: Project Specific

- Compilerz
- Vendor supplied detritus (backdoors?)
- some abandoned python project (OpenLF)
- random abandoned ruby project
- something you write so it can be abandoned in the near future

mmmmm Crosscompilers... fun fun fun. #headache!

For THIS class you want to learn about the RidgeRun ToolChain - http://files.poxlib.org/LeapFrog/RidgeRun-toolchain-369009.tar.bz2
http://elinux.org/LeapFrog_Pollux_Platform:_Build_Environment

Remember the VxWorx memory debugging bugs? https://community.rapid7.com/community/metasploit/blog/2010/08/02/shiny-old-vxworks-vulnerabilities

For THIS class you should become familiar with: https://plus.google.com/communities/116073943758766680750, http://elinux.org/Category:Leapster_Explorer

If you find anything not documented you should give back to those projects, even if you never look back. It could be useful to someone else.

Non English dox?

2.1 Tool chain 설치

2.1.1 Tool chain 풀기

```
$  cd /usr/local
$   cp   $(PackageDir)/4.3.2-eabi-arm.tar.bz2   .
$  sudo  tar  jxvf  4.3.2-eabi-arm.tar.bz2
```

위의 명령어를 실행하면 /usr/local directory에 4.3.2-eabi-arm directory가 생성된다.

2.1.2 Tool chain 경로지정

또한 CROSS Compiler를 설치하게 되면 홈 디렉토리의 .bash_profile을 수정하여 compiler 경로가 맞게끔 설정해야 한다. 그렇지 않을 경우 compile이 안되는 경우가 발생한다.

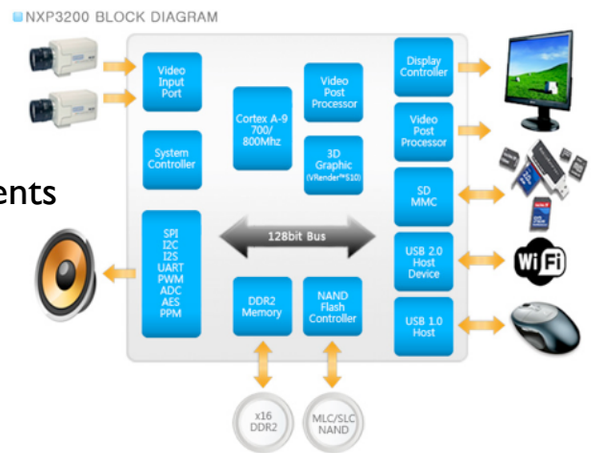
at times you may need to brush up on your Mandarin

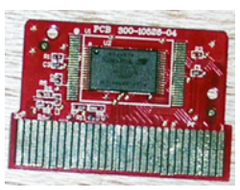
EE Basics and You

plz to JT here

Tell me more

- Resistors / Caps and other basic components
- Main Chip
- Intro to the SoC
- Ram and other storage





We are going to start blending more of the content with things that are applicable to the devices you will be getting in class. You may want to take notes as this stuff is specific to the LeapFrog.

http://wtfmoogle.com/?p=3072
http://nexell.co.kr/kor/pro/pro02.html
http://elinux.org/Leapster_Explorer:_How_To_Make_a_NAND_Cartridge
http://www.elinux.org/LeapFrog_Pollux_Platform:_Cartridge

Lab 1:
Taking things apart

ScrewDriver Time!@

Leapster Time!@#

- Take yours apart
- Take notes
- Identify Chips
- Other artifacts?
- Socialize@!
- Search Twitter?
- Plot on profit!

http://elinux.org/LeapFrog_Pollux_Platform:_Technical_Details
http://www.youtube.com/watch?v=I38FVp08QE8
https://twitter.com/d0tslash
https://twitter.com/m0nk_dot

Goals of Lab 1

- Take the thing apart
- What makes it tick?
- Google for the Docs
- Understand the Docs

- Ask questions!Meet your neighbors
- Try not to break your Leapster on Day 1
- Have Leapster work when reassembled

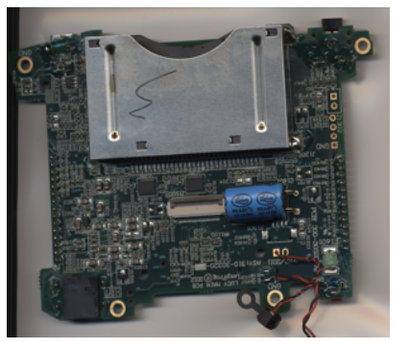
Students should find fun stuff on wtfmoogle, eLinux.org, Nexell chipdocs, references to LF1000 and LF2000 SoC , etc.

someone should realized they share Didj lineage.

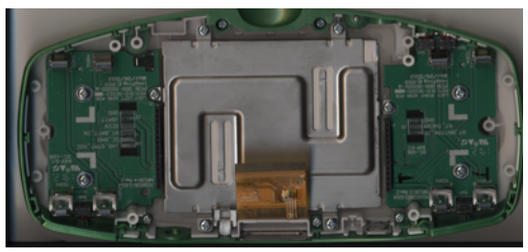
Maybe figure the shell access out instantly?

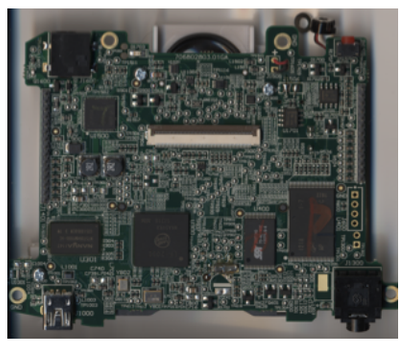
Poxlib IRC logs if they are lucky! http://www.poxlib.org/irclogs/ hell even distant earth may be a long shot - http://blogs.distant-earth.com/wp/?p=64

I'm looking at a PCB



- WTF is this?
- WTF is that?
- Huh?





http://wtfmoogle.com/wp-content/uploads/2013/04/LGBOTTOMHQ.jpg
http://wtfmoogle.com/wp-content/uploads/2013/04/LGSTOPHQ.jpg
http://wtfmoogle.com/wp-content/uploads/2013/04/LGbattHQ.jpg

Did you consider dmesg output ? - http://pastebin.com/Ahk4gUrt
I see a few CL245a's - http://www.ti.com/lit/ds/symlink/sn74cbtlv3245a.pdf
NFJK? - http://www.ti.com/lit/ds/symlink/tpd4s009.pdf
nanya nt5tu64m16gg-ac - http://www.nanya.com/NanyaAdmin/GetFiles.ashx?ID=845
LF-P200 - http://www.poxlib.org/irclogs/didj.log.20130405_pg1.html (audio SoC? lfp100?)
"Custom Audio Chip" - http://elinux.org/LeapFrog_Pollux_Platform:_Technical_Details
LF-2000 - Actually NXP3200 - "arch/arm/mach-nxp3200/soc/sysfs.c:lf2000_sysfs_probe.797 end"
"bma_detect: BMA220 device found" in dmesg - where the fuck is it? Anyone see it?

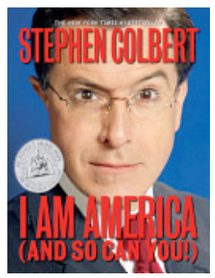
Getting Connected:

JTAG, ICE, SPI & other Acronym Soup

What does this chip support? Why do we care? http://nexell.co.kr/kor/pro/pro02.html

TODO: Generically explain signals, timing, state machine, etc.

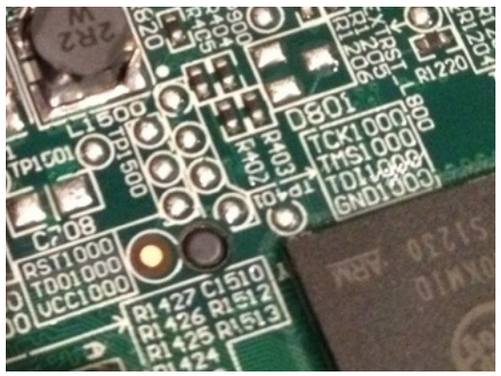
Building Hardware while testing hardware

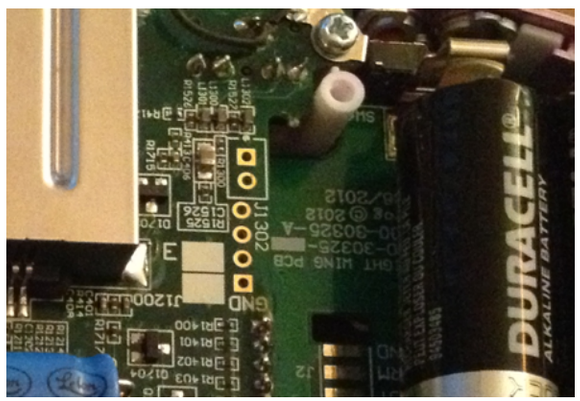


- Designers need JTAG
- Designers need beds of nails
- Designers need to disable / enable things
- I am JTAG (and so can you!)

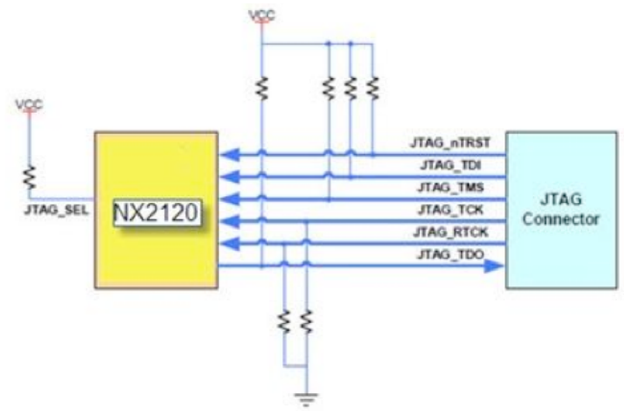
plz to explain SPI, etc. here (KF)

The PCB and pads



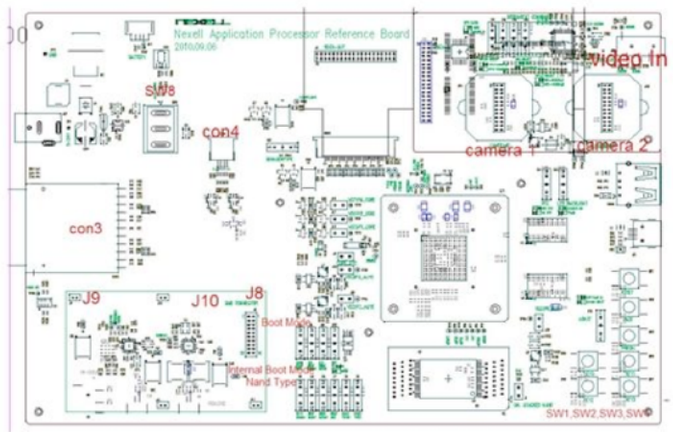


hopefully these caught your eye while you were examining your devices.
Respectively they are JTAG and UART interfaces.



Chipdocs are impossible to find &
"Confidential and Propritary"

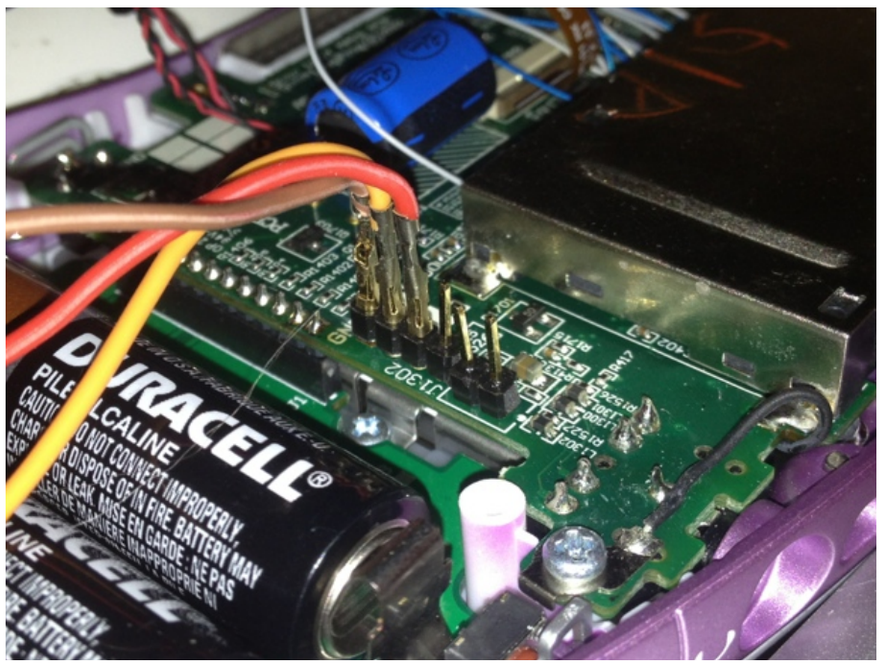
This is as close as I have gotten to documentation for the NXP3200
http://mentodesign.files.wordpress.com/2011/10/nx2120_evk.pdf
http://mentodesign.files.wordpress.com/2011/10/nxp2120datasheetver0-90_work111.pdf



I can Haz NXP3200-EVK?

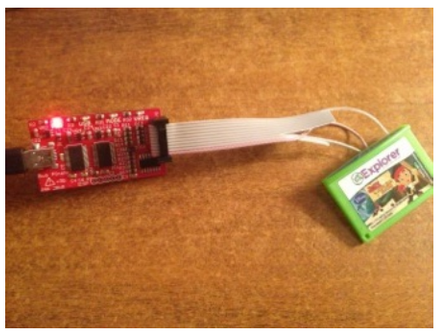
Impossible to find... it is confidential yo!

nailed it!



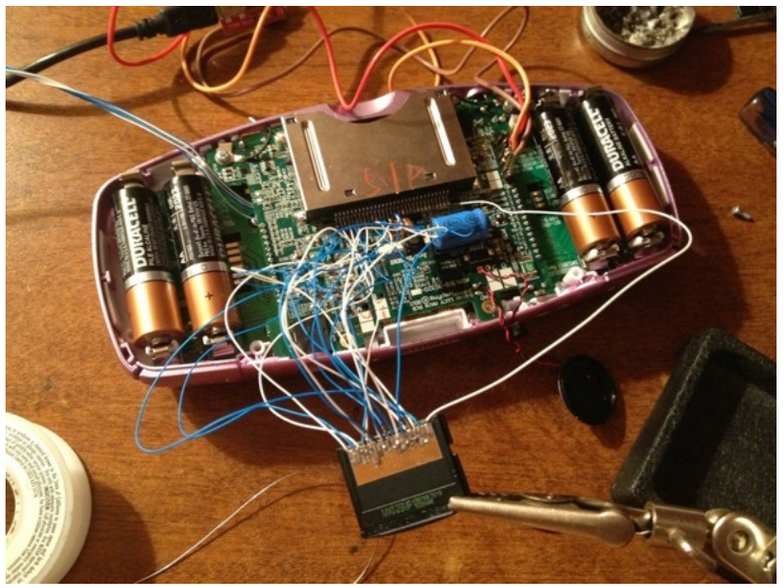
We used some standard header pins as a ‘nail’ to access the through hole debug port.

Tapped it!



You should have been here already! - http://www.elinux.org/LeapFrog_Pollux_Platform:_Cartridge
We will circle back though, don't worry!

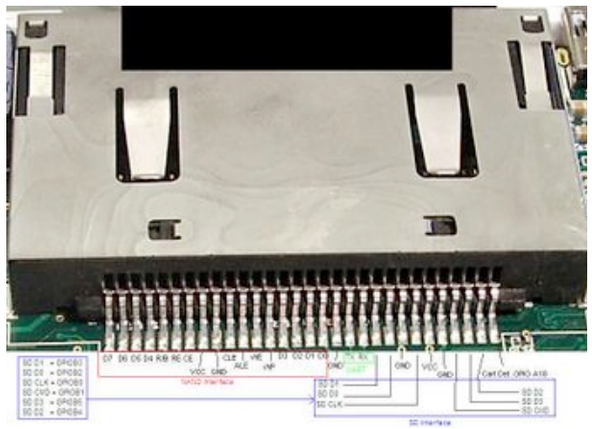
Ummmm made spaghetti... Don’t ask?!

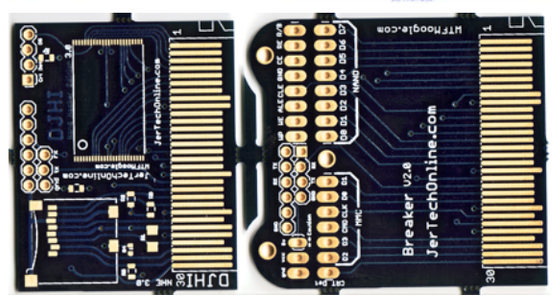


This ultimately helped me understand the Cart inserted GPIO logic, however it ultimately did not lead me where I wanted to go. The leappad would reset every time I applied VCC to the chip. Technically an xD card should give me some NAND love.

Fun signals exposed on your Leapster...

- NAND
- SD
- UART
- Cart Detection
- Bootloader
- USB Serial





http://wtfmoogle.com/?p=1485
https://sites.google.com/site/claudeschwarz/didjhacking2
https://sites.google.com/site/claudeschwarz/didjcart.pdf

WTF does it all mean

- Iterate through the various debug channels
- Pro/Con
- Hardware to make life easy
- Intro GoodFet
- Back in MY day we soldered our own GoodFET@!

understand that Travis hates you... he wants you to learn from your failures. Don't believe me? Mail him, he will have PCBs for you. Order the BOM, torture yourself!
http://www.flickr.com/photos/travisgoodspeed/
http://travisgoodspeed.blogspot.com
https://twitter.com/travisgoodspeed
http://goodfet.sourceforge.net
http://www.adafruit.com/blog/2013/02/28/new-product-goodfet-v42-by-travis-goodspeed-v4-2/
http://www.seeedstudio.com/wish/goodfet-41-jtag-bus-pirate-goodness-all-in-one-p1688
https://exploithub.com/hardware/goodfet-42.html
http://www.riverloopsecurity.com/projects.html
http://rmspeers.com/contact/pcb-requests
http://int3.cc/products/facedancer21

Lab 2:
Talking to things &
Copying shit...

FTDI Serial shell exercise...

Quick Soldering Lesson.

More meet and greet.

Plot on stealing a Cart.

Goals of Lab 2

- Get FTDI working on your computer
  - Note: if you finish quickly help your neighbors
- Used Linux before? If not this should be fun
- If so... go explore, you may be surprised
- Dump the firmware with the aid of serial?
- Dump a cart... screw it dump all the carts!
- Bored? learn yourself to FTDI JTAG bitbang

For a com port - http://www.ftdichip.com/Drivers/VCP.htm
For direct access like Bit Bang - http://www.ftdichip.com/Drivers/D2XX.htm
Bit Bang Modes app note - http://www.ftdichip.com/Support/Documents/AppNotes/AN_232R-01_Bit_Bang_Mode_Available_For_FT232R_and_Ft245R.pdf
Understanding Bitbang mode - http://hackaday.com/2009/09/22/introduction-to-ftdi-bitbang-mode/
DIDJ FTDI JTAG howto - http://elinux.org/LeapFrog_Pollux_Platform:_FTDI_JTAG_How_To
DIDJ Open OCD - http://elinux.org/Didj_JTAG_How_To

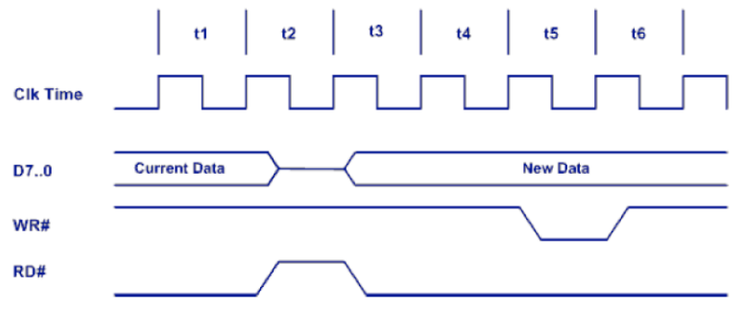
Bang Bang!

3 Synchronous Bit Bang Mode

Synchronous Bit Bang mode is the same as the FT2232 Synchronous Bit Bang mode. With Synchronous Bit Bang mode, data will only be sent out if there is space in the device for data to be read from the pins. This Synchronous Bit Bang mode will read the data bus pins first, before it sends out the byte that has just been transmitted. It is therefore 1 byte behind the output and so to read the inputs for the byte that you have just sent, another byte must be sent.
For example:

- Pins start at 0xFF
- Send 0x55, 0xAA
- Pins go to 0x55 and then to 0xAA
- Data read = 0xFF, 0x55
- Pins start at 0xFF
- Send 0x55, 0xAA, 0xAA (repeat the last byte sent)
- Pins go to 0x55 and then to 0xAA
- Data read = 0xFF, 0x55, 0xAA

The timing for Synchronous Bit bang is described in this diagram and the table below:



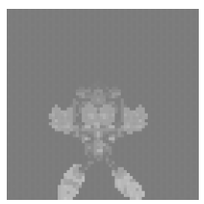
FTDI bitbang docs - http://www.ftdichip.com/Support/Documents/AppNotes/AN_232R-01_Bit_Bang_Mode_Available_For_FT232R_and_Ft245R.pdf
http://elinux.org/LeapFrog_Pollux_Platform:_FTDI_JTAG_How_To

Blob o’ Junk

You are lucky... most of THIS blob of junk is just a common Linux file system.
You should be figuring out how the pieces and parts work. You should have noticed that strace, gdb, strings and friends are already installed...
Plot and scheme.
Find targets.

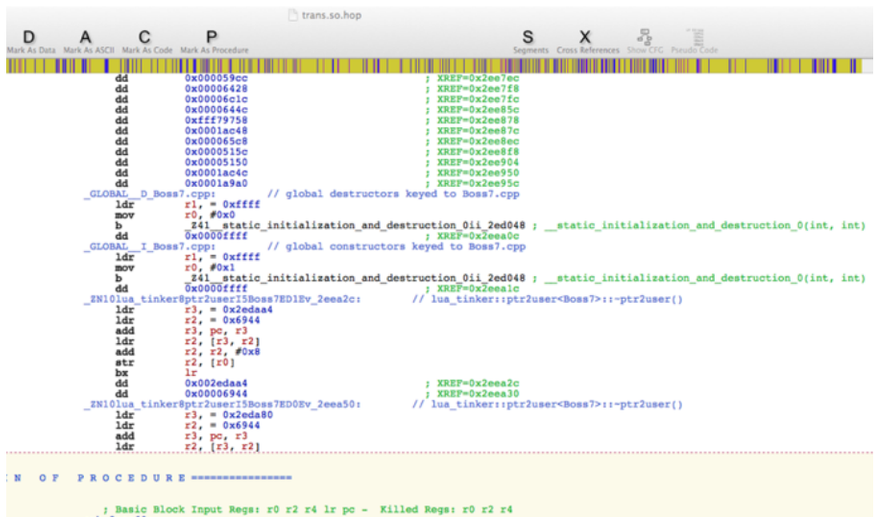
Firmware and You

- Post the the firmware from Lab 2
- Guided walkthrough of the firmware (we can't expect IDA on everyone's machine...)
- We have it... now what?
- Can we modify it?



how does a Cart work?
App.so explaination.
.tex files?
.anim files?
http://elinux.org/Didj_Replacement_App_Menu
http://pastebin.com/j1LUKS7x
http://www.leapfrog.com/gaming/documents/Didj_Custom_Gaming_System-fact_sheet.pdf
"Brio: Firmware is building an abstraction layer (called Brio) to make OS and hardware transparent to developers. This means all software must be ported to Brio to run on this device. "
The LHIC - Leaping Hedgehog Image Converter - http://forums.sonicretro.org/index.php?showtopic=18687&st=75&p=427580&#entry427580
Old DIDJ hacker for image files - http://pastebin.com/ESza2Eq9
Old ROMS?! - http://forums.sonicretro.org/index.php?showtopic=18687&st=45
Check out the sonic images! http://forums.sonicretro.org/index.php?showtopic=18687&st=60&p=426123&#entry426123

App.so Disassembly


trans.so.hop
D Mark As Data
A Mark As ASCII
C Mark As Code
P Mark As Procedure
S Segments
X Cross References
Show CFG
Pseudo Code
dd 0x000059cc ; XREF=0x2ee7ec
dd 0x00006428 ; XREF=0x2ee7f8
dd 0x00006c1c ; XREF=0x2ee7fc
dd 0x0000644c ; XREF=0x2ee85c
dd 0xfff79758 ; XREF=0x2ee878
dd 0x0001ac48 ; XREF=0x2ee87c
dd 0x000065c8 ; XREF=0x2ee8ec
dd 0x0000515c ; XREF=0x2ee8f8
dd 0x00005150 ; XREF=0x2ee904
dd 0x0001ac4c ; XREF=0x2ee950
dd 0x0001a9a0 ; XREF=0x2ee95c
_GLOBAL__D_Boss7.cpp: // global destructors keyed to Boss7.cpp
ldr r1, = 0xffff
mov r0, #0x0
b _Z41__static_initialization_and_destruction_0ii_2ed048 ; __static_initialization_and_destruction_0(int, int)
dd 0x0000ffff ; XREF=0x2eea0c
_GLOBAL__I_Boss7.cpp: // global constructors keyed to Boss7.cpp
ldr r1, = 0xffff
mov r0, #0x1
b _Z41__static_initialization_and_destruction_0ii_2ed048 ; __static_initialization_and_destruction_0(int, int)
dd 0x0000ffff ; XREF=0x2eea1c
_ZN10lua_tinker8ptr2userI5Boss7ED1Ev_2eea2c: // lua_tinker::ptr2user<Boss7>::~ptr2user()
ldr r3, = 0x2edaa4
ldr r2, = 0x6944
add r3, pc, r3
ldr r2, [r3, r2]
add r2, r2, #0x8
str r2, [r0]
bx lr
dd 0x002edaa4 ; XREF=0x2eea2c
dd 0x00006944 ; XREF=0x2eea30
_ZN10lua_tinker8ptr2userI5Boss7ED0Ev_2eea50: // lua_tinker::ptr2user<Boss7>::~ptr2user()
ldr r3, = 0x2eda80
ldr r2, = 0x6944
add r3, pc, r3
ldr r2, [r3, r2]
N OF PROCEDURE ==========
; Basic Block Input Regs: r0 r2 r4 lr pc - Killed Regs: r0 r2 r4

```
LeapFrog::Brio::kPermissionDeniedErr
LeapFrog::Brio::kBadAddressErr
LeapFrog::Brio::kBlockDeviceRequiredErr
LeapFrog::Brio::kDeviceOrResourceBusyErr
LeapFrog::Brio::kFileExistsErr
LeapFrog::Brio::kCrossDeviceLinkErr
LeapFrog::Brio::kNoSuchDeviceErr
LeapFrog::Brio::kNotDirectoryErr
LeapFrog::Brio::kIsDirectoryErr
LeapFrog::Brio::kFileTableOverflowErr
LeapFrog::Brio::kTooManyOpenFilesErr
LeapFrog::Brio::kNotTypewriterErr
LeapFrog::Brio::kTextFileBusyErr
LeapFrog::Brio::kFileTooLargeErr
LeapFrog::Brio::kNoSpaceLeftOnDevice
LeapFrog::Brio::kIllegalSeekErr
LeapFrog::Brio::kReadOnlyFileSystemErr
LeapFrog::Brio::kTooManyLinksErr
LeapFrog::Brio::kBrokenPipeErr
```

IDA alternatives? - http://reverseengineering.stackexchange.com/questions/1817/is-there-any-disassembler-second-to-ida
Analyzing binaries with Hopper - http://abad1dea.tumblr.com/post/23487860422/analyzing-binaries-with-hoppers-decompiler

Lab 3:
Runtime Analysis

I'm gonna suggest you strace ALL the things.
Would it be nice to have a more persistent shell?
Lets walk through getting these things on the internet *FIRST*.
Are you a fancy pants? have a remote arm debugger for IDA pro?

Goals of Lab 3

- Pitch a tent and camp out on the Leapster
- Persistent connection & dev workspace
- We pulled the firmware, now lets look at runtime interactions
- If we change this, it does that...
- What are the key components
- Can we play copied games yet?!

Document the Linux OS, what hardware is this? /sys/devices/system/board/
The lCD is a GiantPlus ILI9322 SPI display - http://en.qi-hardware.com/wiki/Giantplus_TFTs
(`init_lucy: Lucy GPIO mapping`
1. `spi_lcd_init: spi_channel: 0, gpio_port:1, gpio_pin:12, lcd: GiantPlus-1, type: 1)`

Discover the world of MD5 Sums
Wait the Cartridges are One Time Program NAND?
What makes the system say “Hey I have a Cart, it is valid, I’ll let you run it”?
^--- how can you augment that process?
We mentioned strace in a previous slide... did you use it?

LAB3: What kind of hardware is this?

kevinfinisterre — screen — 87×28

```
/sys/devices/system/board # ls
lcd_mfg          lcd_size         platform         system_rev
lcd_mfg_get      lcd_type         platform_family
/sys/devices/system/board # cat *
GiantPlus-1
GiantPlus-1
320x240
ILI9322
LUCY
LEX
0x209
/sys/devices/system/board # cat /proc/cpuinfo
Processor       : ARMv7 Processor rev 2 (v7l)
BogoMIPS        : 1097.72
Features        : swp half thumb fastmult vfp edsp vfpv3 vfpv3d16
CPU implementer : 0x41
CPU architecture: 7
CPU variant     : 0x2
CPU part        : 0xc09
CPU revision    : 2

Hardware        : nxp3200
Revision        : 0x0209
Serial          : 0x0000000000000000
```

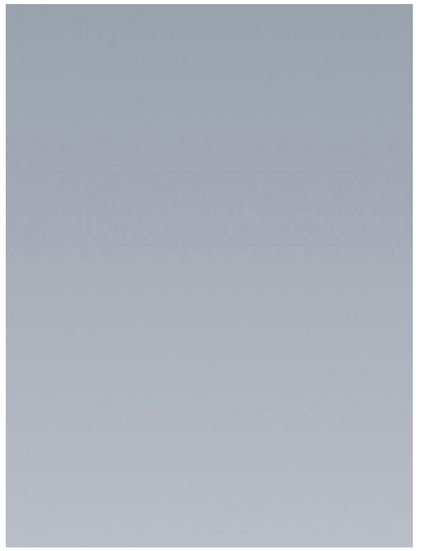
kevinfinisterre — screen — 68×11

```
~ # dmesg | grep nxp
Machine: nxp3200
cpu: nxp3200: NONE Frequency Configuration :
nxp3200-l2k : done board initialize ...
arch/arm/mach-nxp3200/soc/sysfs.c:lf2000_sysfs_probe.791 start
arch/arm/mach-nxp3200/soc/sysfs.c:lf2000_sysfs_probe.797 end
~ #
```

We already knew it was an NXP3200 from elinux.org but this confirms it.
it is ARM, can you emulate it? (we have not)

LAB3: How do I get better access?

- USB networking
- Class USB hub?
- LAN PARTY!@#
- vsftpd?
- telnet?



get your OS USB ethernet stack happy... we use 1.2.3.4 and 1.2.3.5 for addresses
I guess we could have a single linux bastion host and a USB hub?
vsftpd just works... start it.
telnet? hrrrrrrm what to do with no /bin/login or /bin/passwd? why doesn't telnet have a valid pty ?
struggle on it... then we will tell you the answer.

LAB3:WHY md5?

- integrity?
- validation?
- '-rw-r--r--' for root

```
/LF/Bulk # ls /mfgdata
BULK.md5        KERNEL.md5      NorStatus       partitions.md5
EROOTFS.md5     NOR.md5         button.counts
/LF/Bulk # head /mfgdata/*md5
==> /mfgdata/BULK.md5 <==
96468992,121d4ce0ce0d5f08abab9810372bfbfc

==> /mfgdata/EROOTFS.md5 <==
53477376,b25188530114c9e3cf6697ca9aa36c34

==> /mfgdata/KERNEL.md5 <==
2253104,79f0a4ee2ed701cc7faa97b856203c2b

==> /mfgdata/NOR.md5 <==
429712,9d19f64d9c4ec29e8ef7aee40d853f0a

==> /mfgdata/partitions.md5 <==
79f0a4ee2ed701cc7faa97b856203c2b  ./4,2253104,kernel.bin
121d4ce0ce0d5f08abab9810372bfbfc  ./6,96468992,C2G-E1M-W4K-bulk.ubi
8368b6c86c8dedee40e50723ccb063f3  ./meta.inf
9d19f64d9c4ec29e8ef7aee40d853f0a  ./NORBoot/0,429712,u-boot.bin
b25188530114c9e3cf6697ca9aa36c34  ./5,53477376,C2G-E1M-W4K-erootfs.ubi
/LF/Bulk #
```

Nothing too special... just take note that it exists. Plot on it. Will it be a problem?

LAB3: app, AppManager, VideoDaemon, and 'Brio'?

- What do they do!?
- Is this all Flash based?
- Wait is there QT?

```
+++ AppManager: End Load DidjPatches: 2889.65 2656.81
get temp restart player id = 0
+++ AppManager: Bgn Set Profile Logging: 2889.65 2656.81
[0xf] fopenAtomic(/LF/Bulk/settings.cfg) returning 0x0002a508
[0xf] fcloseAtomic returning 0
+++ AppManager: End Set Profile Logging: 2889.66 2656.81
[0x1] Found codec: socaudiolfp100, legacy=0
[0x6] ButtonPowerUSBTask: Use tslib
[0x6] LoadTSLib: use_tslib=1, handle=0x200d0, tsl=0x200f0, fd=16
[0x1] set_hwparams: buffer time=128000, size=4096
[0x1] set_hwparams: period time=32000, size=1024
+++ AppManager: End Set Power & USB: 2890.38 2657.36
[0x280] mCurrentTransition = kLoginApp !
[0x1] CallbackThread: starting audio thread 0x3ba98
+++ AppManager: Bgn Load main.swf: 2890.39 2657.36
[0x280] PushApp Start: LUCY/main.swf; LightningBase/Src/AppManager.cpp; 1140; 24068
[0x280] LoadNewApp path = /LF/Base/LUCY/main.swf
[0x280] LoadNewApp: before; /LF/Base/LUCY/main.swf; 1706; 24068
[0x280] LoadNewApp: after ; /LF/Base/LUCY/main.swf; 1812; 23960
[0x280] PushApp Done: LUCY/main.swf; LightningBase/Src/AppManager.cpp; 1142; 23960
+++ AppManager: End Load main.swf: 2890.56 2657.36
+++ AppManager: UI loaded: 2890.56 2657.36
[0x280] mCurrentTransition = kPushApp !
[0x6] AddListener: added listener 0x5b418, total number 2
[0x6] AddListener: added listener 0x5b45c, total number 3
+++ AppManager: Flash: End Construct DidjPlayer: 2890.56 2657.36
[0x5] AllocBuffer: new buf offset 000E1000, length 0004B000
[0x5] CreateHandle: 0x5b768: 320x240 (1280) @ 0x838e1000
[0x5] RegisterLayer: 0x5b768: 320x240 (1280) @ 0x838e1000
[0x5] SetWindowPosition: 0x5b768: 0,0 .. 320,240
[0x5] CreateHandle: 0x5b7e0: 320x240 (1280) @ 0x41a2b008
[0x5] RegisterLayer: 0x5b7e0: 320x240 (1280) @ 0x41a2b008
[0x5] UnRegisterLayer: 0x5b7e0: 320x240 (1280) @ 0x41a2b008
[0x5] RegisterLayer: 0x1a4a0: 320x240 (1280) @ 0x83896000
[0x5] SetWindowPosition: 0x1a4a0: 0,0 .. 320,240
```

strace all the things!
/LF/Bulk # strace -o app_strace -ivfff app >app_launch.log 2>&1

what is in /LF/Base/Brio ? I wonder what /tmp/cart_brio_state is?
Leave the Video Daemon running. Kill app and AppManager. Then manually start AppManager through Strace.

AppMGR output - http://pastebin.com/i0hnm1uR

LAB3: I can haz a.out?

RidgeRun toolkit. - http://files.poxlib.org/LeapFrog/
http://files.poxlib.org/LeapFrog/RidgeRun-toolchain-369009.tar.bz2

Plz to having pwnies?

I bet you are all ready to move on to playing copied games now? Guess what? Tomorrow people... tomorrow!
See ya in the morn.

</First Half>

be sure to take notes on your lunch time hacking! Be mindful of your AA batteries... DON’T break it before you get back from eating. =]

Second Half Schedule

- Soldering all the things
- JT talks USB / NK talks USB
- Lab 4: To Live and Die in LA
- Stories from a Real Life Fab project
- Lab 5: We are persist, now what?
- Techniques for moving beyond n00b
- Lab 6: A dash of pwn sauce...

plz to JT here

Soldering all the things

plz to JT here

You are doing it wrong

- How to solder
- How to desolder
- How to HotAir
- How to PCB
- How to #CharlieSheenWin

plz to JT here

Soldering 101

- Through Hole
- Proper sponge usage / Proper cleaning
- Cutting Traces
- Jumping Resistance
- Watch teh YouTubez for technique!

I'm going to walk you through simple techniques here, live and in person!
Just like writing code or finding bugs, there are a billion ways to do it right.
Really, you just need to practice and get comfortable. I'd suggest buying some broken crap off ebay and just playing a ton.

http://lmgtfy.com/?q=soldering+techniques

Soldering 201

- surface mount... damn you travis
- pro tip: start messy, then clean?

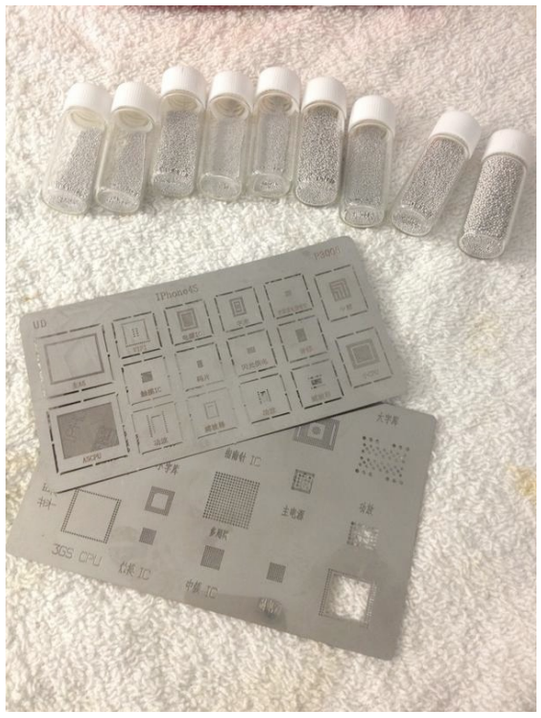
plz to JT here

Soldering 301

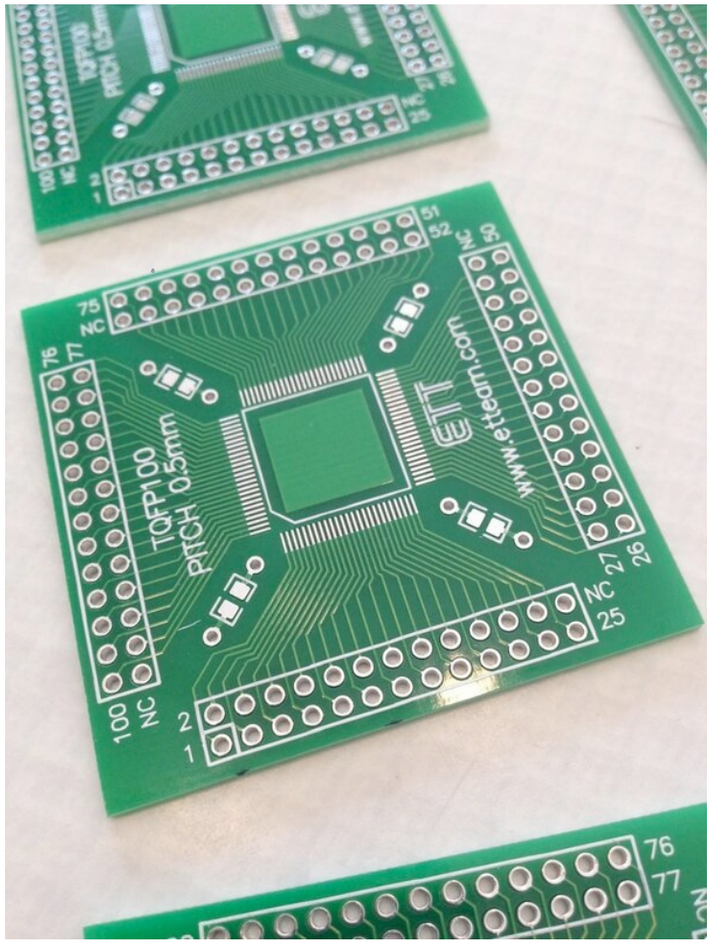
- rake that tsop
- mixing in chip quik!
- BGA?

plz to JT here

Fsck BGA...



Not fun... just not



SchmartBoards!

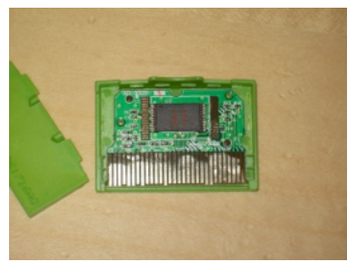
DeSoldering 101

- Learn to use braid
- Learn to use a solder sucker
- Learn to use chip quik

plz to JT here

DeSoldering 201

- Hot air!



plz to JT here

Should we hot air off a leapster cart? Try to transplant one from a USB drive? I brought two USB drives with me...
http://elinux.org/Leapster_Explorer:_How_To_Make_a_NAND_Cartridge
Prelude to the money shot.

DeSoldering 301

- Cleaning the board, cleaning the parts.

plz to JT here

Hardware RE 101

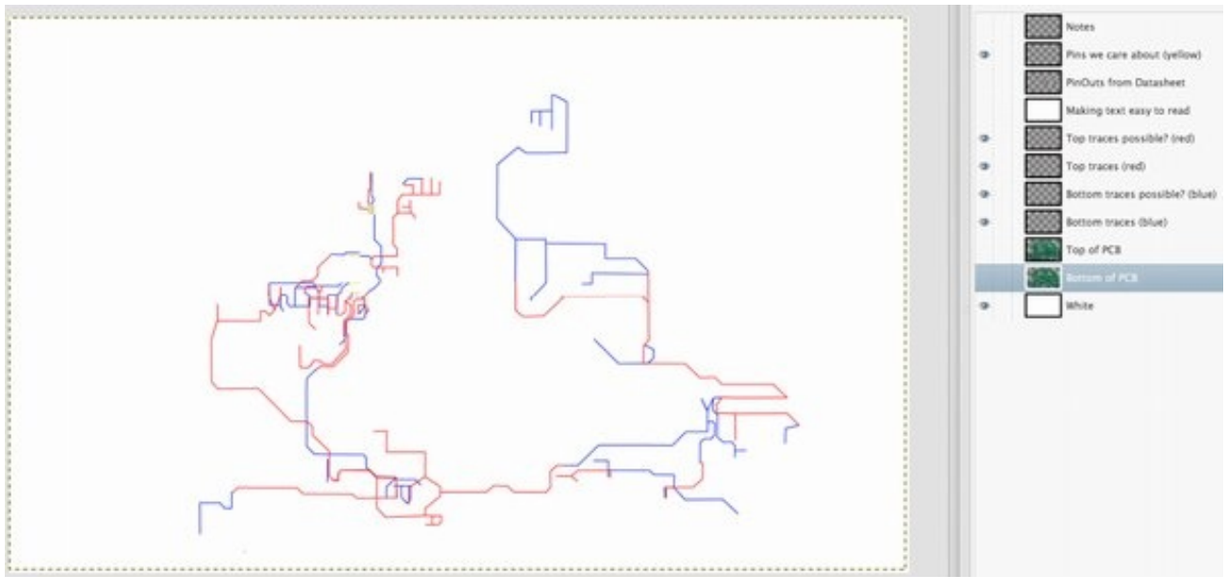
- visual check between pcb and data sheet
- tag n' pop

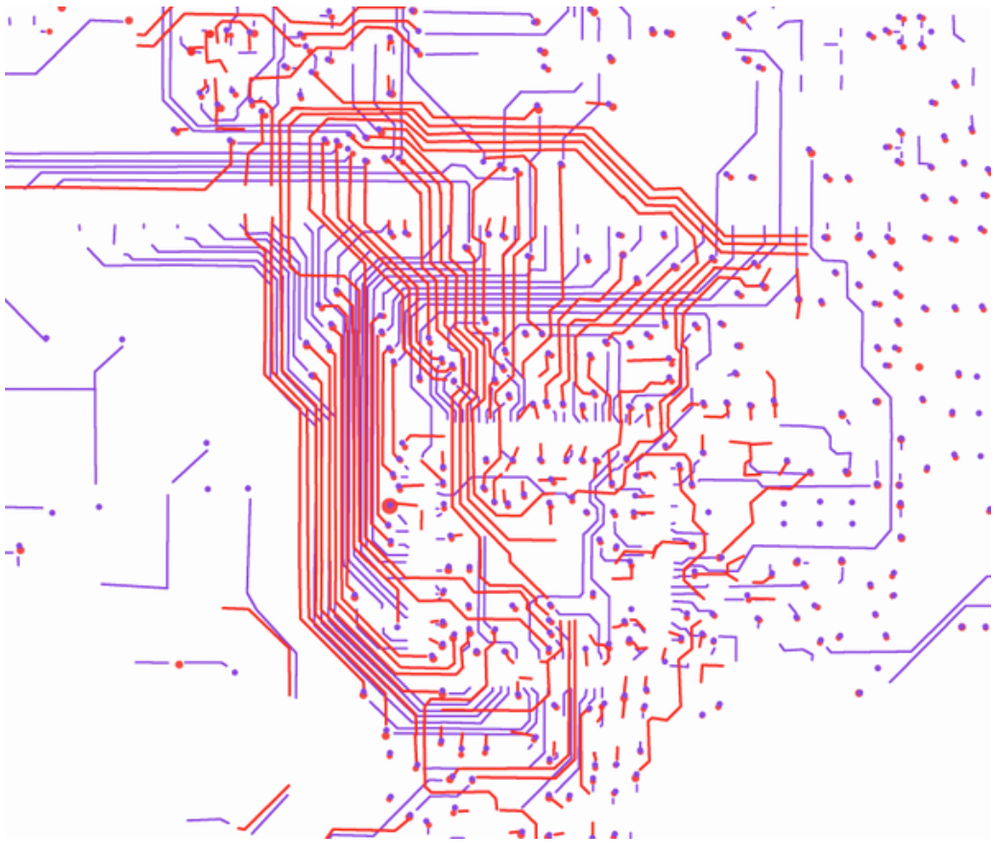
JT / NK to babble here

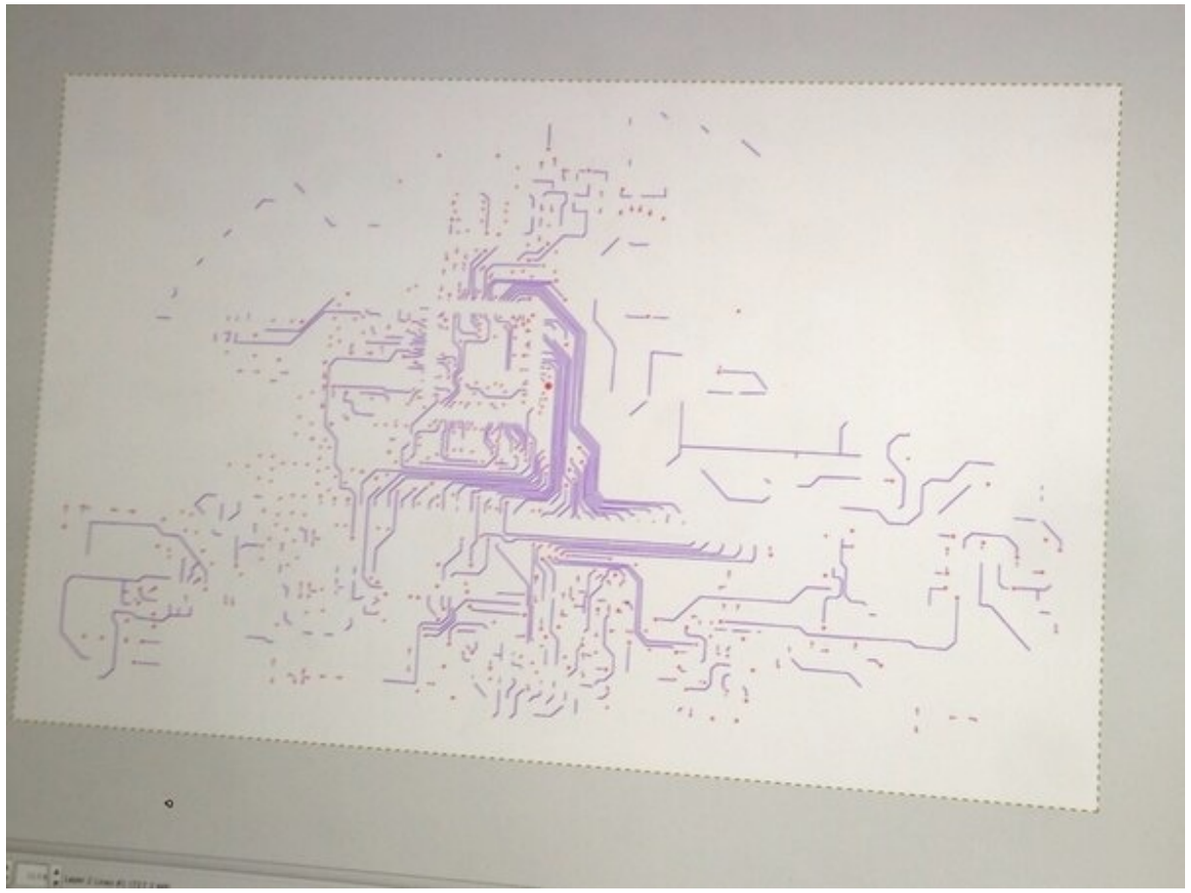
Hardware RE 201

- desolder and scan, tracing in the gimp
- live tagging / dynamic analysis

JT / NK to babble here


Notes
Pins we care about (yellow)
PinOuts from Datasheet
Making text easy to read
Top traces possible? (red)
Top traces (red)
Bottom traces possible? (blue)
Bottom traces (blue)
Top of PCB
Bottom of PCB
White





Hardware RE 301

- Just do it a bunch
- Buy random crap, open it up, figure it out

JT / NK to babble here

The MasterLock DialSpeed 1500 ebdx

http://www.gadgetreview.com/2012/08/masterlock-dialspeed-1500edbx-padlock-review.html

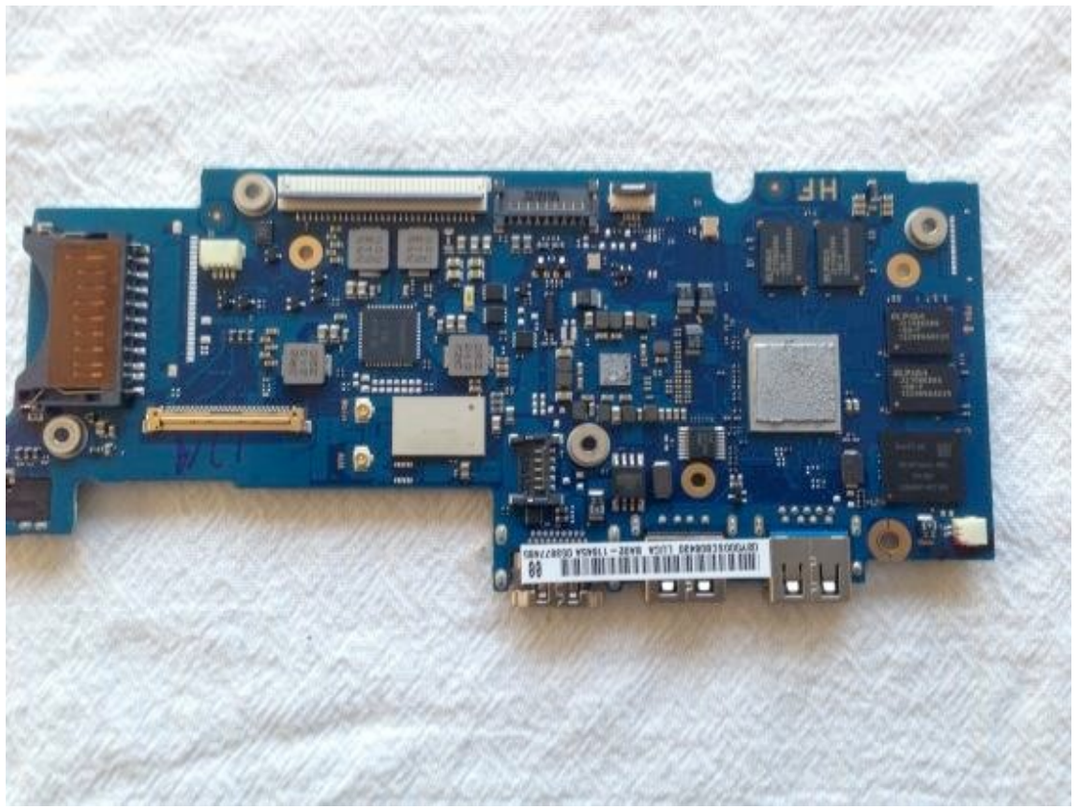
This is what made us decide to teach this class... but we got really bored / sidetracked :)

Magnetic
Project Mat

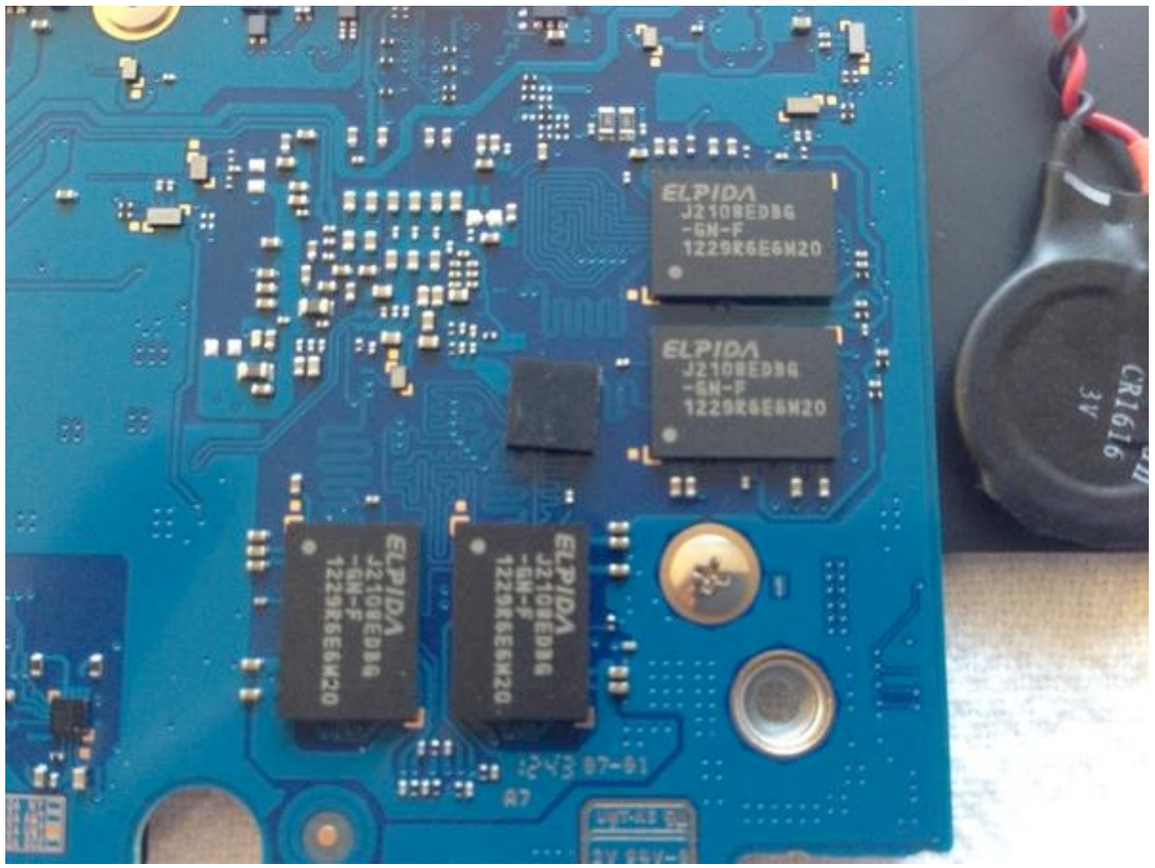
I think this was a Sony Xperia Z... looks like it at least.

Random Android TV Dongle...

Microsoft Surface RT



Samsung ARM (Daisy) Chromebook



Daisy traces!

Hardware RE 401

- disabling hardware anti tamper checks
- enable debug

JT / NK to babble here

Lab 4:
To Live and Die in LA

plz to JT here

Simple guided tutorial on Saleae & USBee LA

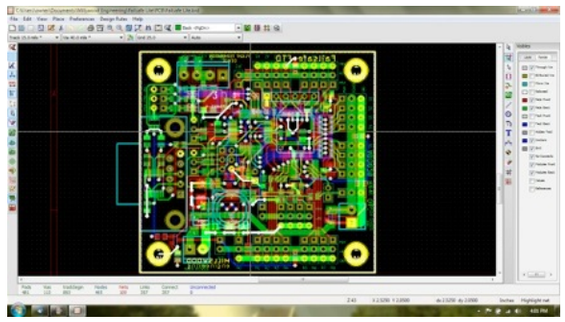
Honestly, we are just going to walk through our Leapster and find the clock and other pins... latch and watch, get used to the interface and let NK school us all :)

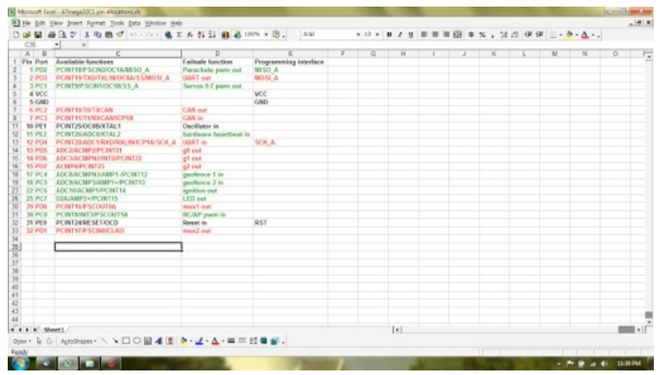
Stories from a Real Life Fab project

Some of you know that I am a full blown quad copter addict. I am not a supporter of the OpenPilot project and helped push out a batch of 500 autopilot boards. Likewise I've also helped design a Failsafe with the folks at Millswood engineering.
(pass around both boards).
http://www.millswoodeng.com.au/failsafe_device.html
http://www.readymaderc.com/store/index.php?main_page=product_info&products_id=1555
http://www.openpilot.org

KF tells a story

- OpelPilot CC3D & Millswood Failsafe Fabrication
- TurnKey Fab Shop
- Tiered sales approach
  - PDB Only
  - You supply BOM vs. Shop supplied BOM
- TurnKey vs. manual testing
- Firmware loading
- Bulk cuts BOM price severely
- Contrast to OSHPark / old DorkBOTPDX





Kicad vs. Eagle debate
Altium
How to colloborate over a distance
Both projectes were with folks in Australia.

FUUUUUUUUUCK testing by hand sucks

Goals for Lab 4

- Time to use a Saleae & / | Bus Pirate

plz to JT here
(Sniff button interactions? SPI Display sniff?)

Lab 5:
We have persist, now what?

easy net access
compiler?
more tools?
steal games?!
homebrew?
UI mod?
Game mod / cheats?
USB OTG to have nasty devices connected? - http://www.harbaum.org/till/n800_usb/index.shtml

How to interwebz?

OSX users can use sysctl, natd and ipfw
Linux users may find it easy to use shorewall
Windows users can fuck off... I mean good luck getting that shit to work!

OSX interwebz

- sysctl enable forwarding
- natd on LAN interface
- ipfw rules for traffic

kevinfinisterre — natd — 96×32

```
Kevins-iMac:~ kevinfinisterre$ sudo sysctl -w net.inet.ip.forwarding=1
net.inet.ip.forwarding: 0 -> 1
Kevins-iMac:~ kevinfinisterre$ sudo natd -interface en0 -v yes
Sep 21 16:44:28 Kevins-iMac.local natd[58844] <Info>: Aliasing to 10.0.1.72, mtu 1500 bytes
In  [TCP]  [TCP] 199.59.148.139:443 -> 10.0.1.72:52887 aliased to
           [TCP] 199.59.148.139:443 -> 10.0.1.72:52887
Out [TCP]  [TCP] 10.0.1.72:52887 -> 199.59.148.139:443 aliased to
           [TCP] 10.0.1.72:52887 -> 199.59.148.139:443
In  [TCP]  [TCP] 199.59.148.241:443 -> 10.0.1.72:51572 aliased to
           [TCP] 199.59.148.241:443 -> 10.0.1.72:51572
Out [TCP]  [TCP] 10.0.1.72:51572 -> 199.59.148.241:443 aliased to
           [TCP] 10.0.1.72:51572 -> 199.59.148.241:443
In  [TCP]  [TCP] 74.125.225.72:443 -> 10.0.1.72:63416 aliased to
           [TCP] 74.125.225.72:443 -> 10.0.1.72:63416
Out [TCP]  [TCP] 10.0.1.72:63416 -> 74.125.225.72:443 aliased to
           [TCP] 10.0.1.72:63416 -> 74.125.225.72:443
In  [TCP]  [TCP] 199.59.148.139:443 -> 10.0.1.72:52954 aliased to
           [TCP] 199.59.148.139:443 -> 10.0.1.72:52954
Out [TCP]  [TCP] 10.0.1.72:52954 -> 199.59.148.139:443 aliased to
           [TCP] 10.0.1.72:52954 -> 199.59.148.139:443
In  [UDP]  [UDP] 10.0.1.71:631 -> 10.0.1.255:631 aliased to
           [UDP] 10.0.1.71:631 -> 10.0.1.255:631
In  [TCP]  [TCP] 199.59.150.41:443 -> 10.0.1.72:63516 aliased to
           [TCP] 199.59.150.41:443 -> 10.0.1.72:63516
Out [TCP]  [TCP] 10.0.1.72:63516 -> 199.59.150.41:443 aliased to
           [TCP] 10.0.1.72:63516 -> 199.59.150.41:443
In  [TCP]  [TCP] 199.59.150.41:443 -> 10.0.1.72:63516 aliased to
           [TCP] 199.59.150.41:443 -> 10.0.1.72:63516
Out [TCP]  [TCP] 10.0.1.72:63516 -> 199.59.150.41:443 aliased to
           [TCP] 10.0.1.72:63516 -> 199.59.150.41:443
In  [UDP]  [UDP] 10.0.1.71:57351 -> 255.255.255.255:2223 aliased to
           [UDP] 10.0.1.71:57351 -> 255.255.255.255:2223
```

kevinfinisterre — bash — 85×23

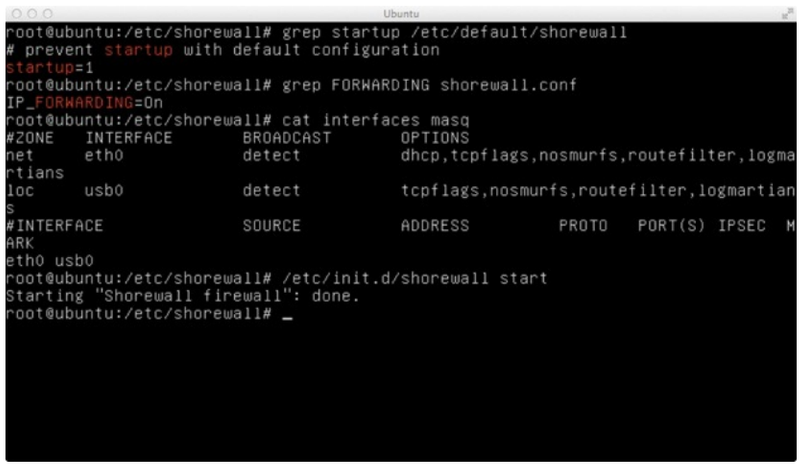
```
Last login: Sat Sep 21 16:39:11 on ttys003
Kevins-iMac:~ kevinfinisterre$ sudo ipfw flush
Are you sure? [yn] y
Kevins-iMac:~ kevinfinisterre$ sudo ipfw add divert natd all from any to any via en0
00100 divert 8668 ip from any to any via en0
Kevins-iMac:~ kevinfinisterre$ sudo ipfw add divert natd all from any to any via en3
00200 divert 8668 ip from any to any via en3
Kevins-iMac:~ kevinfinisterre$ sudo ipfw add 65535 allow all from any to any
65535 allow ip from any to any
Kevins-iMac:~ kevinfinisterre$
```

pull up the usb interface in this case as en3 and use the en0 interface to serve your local connection.

http://david-sundstrom.blogspot.com/2009/10/mac-osx-as-router-ip-forwarding-with.html

Linux Interwebs

- Shorewall
- 2 interfaces config
- Iptables
- Enable forwarding

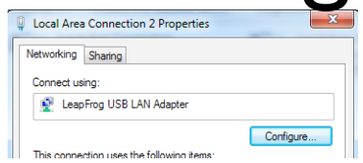


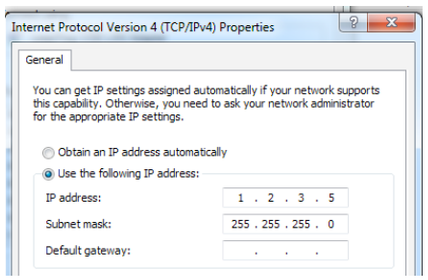
sudo echo 1 > /proc/sys/net/ipv4/ip_forward if you wanna roll manual style.
iptables -F; iptables -t nat -F; iptables -t mangle -F ...
ala - http://www.tldp.org/HOWTO/html_single/Masquerading-Simple-HOWTO/

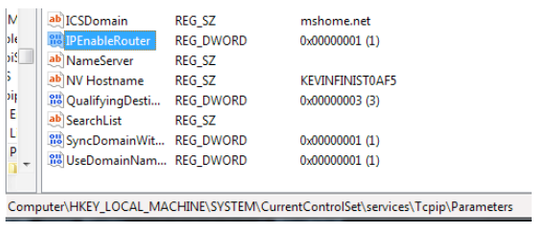
Shorewall - http://www.shorewall.net/two-interface.htm

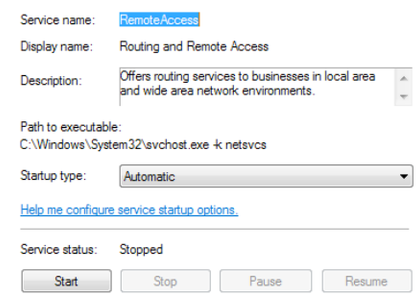
Windows forwarding?

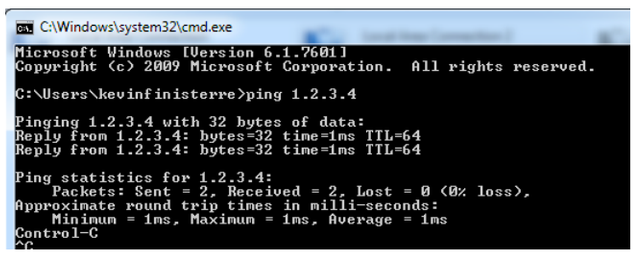
- Tested on Windows 7
- Couldn't make it work
- On Your own....




Internet Protocol Version 4 (TCP/IPv4) Properties
General
You can get IP settings assigned automatically if your network supports this capability. Otherwise, you need to ask your network administrator for the appropriate IP settings.
Obtain an IP address automatically
Use the following IP address:
IP address: 1 . 2 . 3 . 5
Subnet mask: 255 . 255 . 255 . 0
Default gateway:



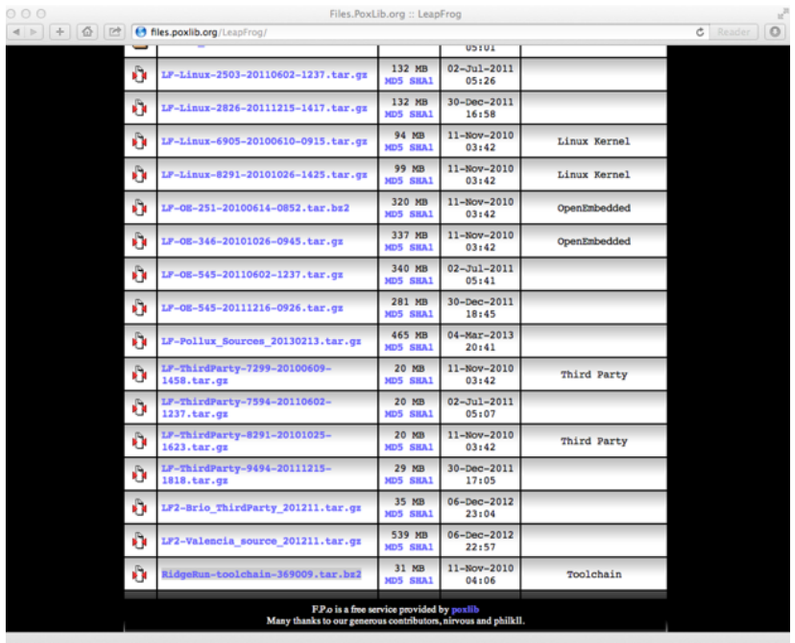



C:\Windows\system32\cmd.exe
Microsoft Windows [Version 6.1.7601]
Copyright (c) 2009 Microsoft Corporation. All rights reserved.
C:\Users\kevinfinisterre>ping 1.2.3.4
Pinging 1.2.3.4 with 32 bytes of data:
Reply from 1.2.3.4: bytes=32 time=1ms TTL=64
Reply from 1.2.3.4: bytes=32 time=1ms TTL=64
Ping statistics for 1.2.3.4:
Packets: Sent = 2, Received = 2, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
Minimum = 1ms, Maximum = 1ms, Average = 1ms
Control-C
^C

http://answers.microsoft.com/en-us/windows/forum/windows_7-networking/how-to-enable-ip-routing-in-windows-7/8970e722-e947-460d-80d5-fd6ffc850f3f

plz to compiling?

- Poxlib RidgeRun Toolchain
- eLinux.org notes
  - Scratchbox?
  - OpenLF Buildroot
  - Devroot? (u-boot)


Files.PoxLib.org :: LeapFrog
files.poxlib.org/LeapFrog/
LF-Linux-2503-20110602-1237.tar.gz 132 MB MD5 SHA1 02-Jul-2011 05:26
LF-Linux-2826-20111215-1417.tar.gz 132 MB MD5 SHA1 30-Dec-2011 16:58
LF-Linux-6905-20100610-0915.tar.gz 94 MB MD5 SHA1 11-Nov-2010 03:42 Linux Kernel
LF-Linux-8291-20101026-1425.tar.gz 99 MB MD5 SHA1 11-Nov-2010 03:42 Linux Kernel
LF-OE-251-20100614-0852.tar.bz2 320 MB MD5 SHA1 11-Nov-2010 03:42 OpenEmbedded
LF-OE-346-20101026-0945.tar.gz 337 MB MD5 SHA1 11-Nov-2010 03:42 OpenEmbedded
LF-OE-545-20110602-1237.tar.gz 340 MB MD5 SHA1 02-Jul-2011 05:41
LF-OE-545-20111216-0926.tar.gz 281 MB MD5 SHA1 30-Dec-2011 18:45
LF-Pollux_Sources_20130213.tar.gz 465 MB MD5 SHA1 04-Mar-2013 20:41
LF-ThirdParty-7299-20100609-1458.tar.gz 20 MB MD5 SHA1 11-Nov-2010 03:42 Third Party
LF-ThirdParty-7594-20110602-1237.tar.gz 20 MB MD5 SHA1 02-Jul-2011 05:07
LF-ThirdParty-8291-20101025-1623.tar.gz 20 MB MD5 SHA1 11-Nov-2010 03:42 Third Party
LF-ThirdParty-9494-20111215-1818.tar.gz 29 MB MD5 SHA1 30-Dec-2011 17:05
LF2-Brio_ThirdParty_201211.tar.gz 35 MB MD5 SHA1 06-Dec-2012 23:04
LF2-Valencia_source_201211.tar.gz 539 MB MD5 SHA1 06-Dec-2012 22:57
RidgeRun-toolchain-369009.tar.bz2 31 MB MD5 SHA1 11-Nov-2010 04:06 Toolchain
F.P.o is a free service provided by poxlib
Many thanks to our generous contributors, nirvous and philkl.

http://files.poxlib.org/LeapFrog/RidgeRun-toolchain-369009.tar.bz2
http://www.ridgerun.com/www/index.php
http://elinux.org/LeapFrog_Pollux_Platform:_Build_Environment
http://elinux.org/Leapfrog_Source_Code
http://elinux.org/Didj_Kernel_Build_Environment
http://elinux.org/Didj_Build_Environment
https://code.jeffkent.net/trac/nc600/wiki/DevrootGuide

Goals of Lab 5

- Play a game w/o the cart in the leapster

There is another variation of this for the Leapster Ultra... it involves DBUS.

I can haz pwnies now?

- What is lfcart.ko ?
- What is cart_brio_state?

```
[407db62c] open("/LF/Cart/", O_RDONLY|O_NONBLOCK
[40823bf4] open("/LF/Cart/TFM/meta.inf", O_RDONL
[40823bf4] open("/LF/Cart/TFM/GameInfo.json", O_
[40823bf4] open("/sys/devices/system/board/plat
[407db62c] open("/LF/Bulk", O_RDONLY|O_NONBLOCK|
[40823bf4] open("/LF/Bulk/LanguagePack_en/meta.
[407db62c] open("/tmp/Cart/", O_RDONLY|O_NONBLO
[40823bf4] open("/LF/Cart/TFM/GAMS/BaseImage.pn
[40823bf4] open("/tmp/Cart//BaseImage.png", O_W
[40823bf4] open("/LF/Cart/TFM/GAMS/GAMS/PopupIc
[40823bf4] open("/tmp/Cart//PopupIcon.png", O_W
[40823bf4] open("/LF/Bulk/ProgramFiles/GAMS-0x0
[40823bf4] open("/LF/Bulk/ProgramFiles/GAMS-0x0
[40823bf4] open("/LF/Bulk/ProgramFiles/PetPad/Ba
[40823bf4] open("/LF/Bulk/ProgramFiles/ConnectMo
[40823bf4] open("/tmp/Cart//BaseImage.png", O_RD
[40823bf4] open("/tmp/cart_brio_state", O_RDONLY
[40823bf4] open("/tmp/cart_brio_state", O_RDONLY
[40823bf4] open("/tmp/cart_brio_state", O_RDONLY
[40823bf4] open("/tmp/cart_brio_state", O_RDONLY
[40823bf4] open("/LF/Bulk/Data/Local/0/./profile
[40823bf4] open("/LF/Bulk/Data/Local/0/./profile
[40823bf4] open("/LF/Bulk/Data/Local/0/./profile
[40823bf4] open("/LF/Bulk/Data/Local/0/./profile
[40823bf4] open("/tmp/cart_brio_state", O_RDONLY
[40823bf4] open("/tmp/cart_brio_state", O_RDONLY
[40823bf4] open("/tmp/cart_brio_state", O_RDONLY
[40823bf4] open("/tmp/cart_brio_state", O_RDONLY
```

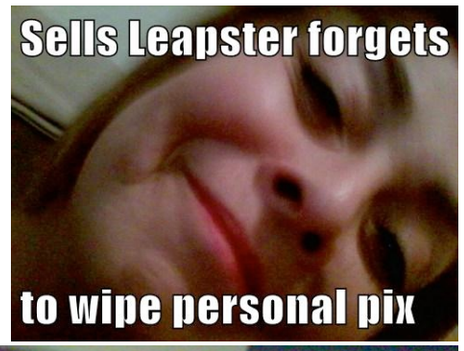
While sniffing AppManager with strace I noticed /tmp/cart_brio_state

Look Ma, no cart!

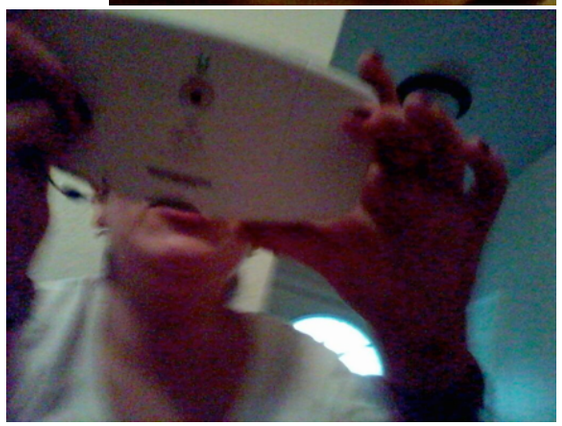
- /LF/Cart/lib/libUtility.so
- /tmp/cart_brio_state
- CARTRIDGE_STATE_INSERTED
- just remove lfcart.ko

There will me a Red X over your Cart when you start…
~ # rmmod lfcart
cd /LF/Cart and untar the game.
~ # echo "3, CARTRIDGE_STATE_SUCKMYBALLS" > /tmp/cart_brio_state
Icon will either turn solid green show the game icon on main page. Touch it..

Anything else on here?



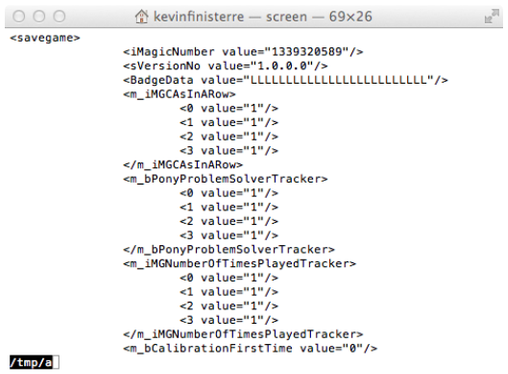
- LeapsterGS forensics? lol
- Pix on used devices
- Free games!?
- Savegame.bin & friends



Buy a broken one on eBay and start looking in /LF/Bulk/Data/Local/
Start to lulz

help your kid cheat?
Badges, Micromods, etc.

- .DAT
- .BIN
- .XML
- .jexon
- MagicNumber?



I have no clue what the format of the Savegame files, Micromods or Badges are...
have fun!
Teach your kid to win like Charlie Sheen!

Techniques for moving beyond n00b

plz to JT here

tricks of the trade

- Hot Air a PCB, trace with the Gimp
- Development Boards
- Enabling debug / bypassing hardware protections
- Moar content here

Circle back and mention the Nexell dev board...

Lab 6:
A dash of pwnsauce...

Goals of Lab 6

- End game / time to show off
- Edit that fucking ROM to full on pwnium
- Have fun, break stuff On-The-Go?

the end is near...

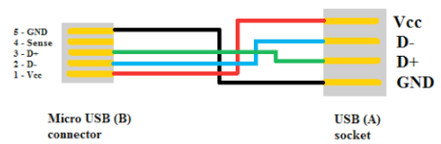
NastyCartTime?

- Notice /lib on the carts?
- Malicious App.so?
- Cart full of ROMs?
  - swap active ROM?

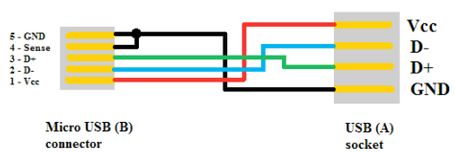
http://elinux.org/Didj_Make_ATAP
http://elinux.org/LeapFrog_Pollux_Platform:_Cartridge

USB On-The-Go?!@

- USB toys?
- RF gear?
- more space?
- Female USB A
- Male mini-B



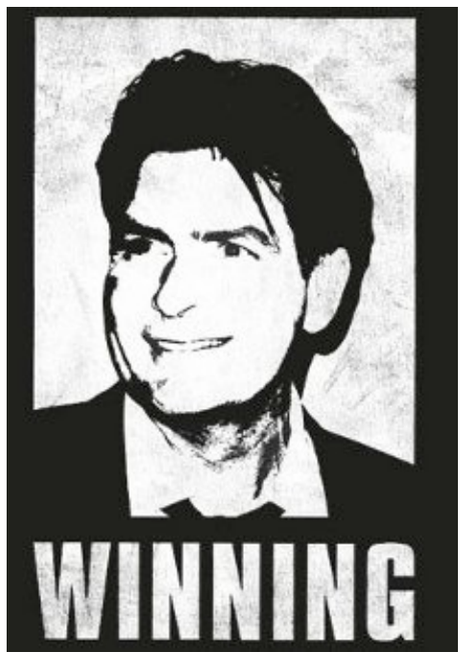
If you want to use it for working OTG adapter you have to connect the micro usb connector 4. pin to GND (5. pin).
Like this:



Y U NO SELL THIS CABLE@#$
http://forum.xda-developers.com/showthread.php?p=14469942
http://www.harbaum.org/till/n800_usb/index.shtml

Math Game?

- 2 + 2 = 5
- Get your learn on!



OMG Pop Quiz

- Best way to solder surface mount TSOP
  - A: Rake
- How long was Rick Ross a prison guard?
  - A: What do you mean? Freeway Ricky, or Ricky Rosey? Auuuuuuuugh!!@
- Who is more awesome (KF | JT|NK)
  - $ ruby -e 'p ["KF", "JT","”NK”].choice'

https://twitter.com/d0tslash/status/380410472924594176
http://www.hiphopdx.com/index/news/id.7847/title.rick-ross-admits-correctional-officer-past
http://www.imdb.com/title/tt0071853/quotes

</Second Half>

fin(isterre)

http://en.wikipedia.org/wiki/Finistère

thanks for p(l)aying

http://rapgenius.com/50707/Wu-tang-clan-cream/Dolla-dolla-bill-yall